TESIS - KS142501

ANALISIS KONSISTENSI HASIL RISIKO TEKNOLOGI INFORMASI *FAILURE MODE AND EFFECT ANALYSIS (FMEA)*

NINA FADILAH NAJWA
NRP. 05211650012003

DOSEN PEMBIMBING:
DR. APOL PRIBADI SUBRIADI, S.T., M.T.
NIP. 197002252009121001

PROGRAM MAGISTER
DEPARTEMEN SISTEM INFORMASI
FAKULTAS TEKNOLOGI INFORMASI DAN KOMUNIKASI
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
SURABAYA
2018

TESIS - KS142501

CONSISTENCY ANALYSIS OF INFORMATION TECHNOLOGY RISK RESULT BY FAILURE MODE AND EFFECT ANALYSIS (FMEA)

NINA FADILAH NAJWA
NRP. 05211650012003

SUPERVISOR:
DR. APOL PRIBADI SUBRIADI, S.T., M.T.
NIP. 197002252009121001

PROGRAM MAGISTER
DEPARTEMEN SISTEM INFORMASI
FAKULTAS TEKNOLOGI INFORMASI DAN KOMUNIKASI
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
SURABAYA
2018

LEMBAR PENGESAHAN TESIS

LEMBAR PENGESAHAN TESIS

Tesis disusun untuk memenuhi salah satu syarat memperoleh gelar
Magister Komputer (M.Kom)
di
Institut Teknologi Sepuluh Nopember
Oleh:

Nina Fadilah Najwa
NRP.05211650012003

Tanggal Ujian : 18 Juli 2018
Periode Wisuda : September 2018

Disetujui oleh:
Dr. Apol Pribadi Subriadi, S.T., M.T.
NIP. 19700225 2009121001 (Pembimbing)

Tony Dwi Susanto, S.T., M.T., Ph.D.
NIP. 19751211 2008121001 (Penguji 1)

Faizal Mahananto,S.Kom., M.Eng., Ph.D.
NIK. 5200201301010 (Penguji 2)

Dekan
Fakultas Teknologi Informasi dan Komunikasi

Dr. Agus Zainal Arifin, S.Kom., M.Kom
NIP. 19720809 199512 1 001

i

ANALISIS KONSISTENSI HASIL RISIKO TEKNOLOGI INFORMASI

***FAILURE MODE AND EFFECT ANALYSIS* (FMEA)**

Nama Mahasiswa : Nina Fadilah Najwa
NRP : 05211650012003
Dosen Pembimbing : Dr. Apol Pribadi Subriadi, S.T, M.T

ABSTRAK

Failure Mode and Effect Analysis (FMEA) merupakan salah satu metode dalam manajemen risiko yang dapat digunakan dalam berbagai bidang seperti industri manufaktur dan jasa, organisasi profit dan non profit, organisasi *private*, publik, ataupun organisasi pemerintahan. Beberapa penelitian mengkritisi metode FMEA karena terdapatnya limitasi atau kelemahan dari penggunaan FMEA terutama pada isu konsistensi. Jika FMEA digunakan secara tidak tepat atau terdapatnya hasil yang tidak konsisten, akan memberikan kerugian pada organisasi. Hal ini dikarenakan, prioritas risiko membutuhkan biaya yang lebih besar pada risiko peringkat tertinggi. Perbedaan peringkat risiko tersebut dapat terjadi kesalahan dalam pencegahan atau fokus penanganan. Tujuan dari penelitian ini adalah untuk memberikan kontribusi penelitian dengan mensintesis kerangka FMEA untuk meminimalisir isu konsistensi dan subjektifitas dalam manajemen risiko.

Penelitian ini menggunakan dua siklus *action resereach* (*plan, act, observe, reflect*). Siklus pertama pada *action research* untuk menguji dan membuktikan konsistensi FMEA Tradisional. Tahapan dalam analisis konsistensi adalah dengan menganalisa risiko TI oleh dua tim yang berbeda pada studi kasus yang sama. Perbedaan peringkat risiko yang dilakukan oleh kedua tim akan dianalisis kesenjangannya dan diberikan usulan perbaikan. Kemudian dilanjutkan dengan siklus *action research* yang kedua, yaitu untuk mengimplementasikan kerangka FMEA yang telah disintesiskan. Tahapan awal dengan melakukan sintesis kerangka FMEA yang diperbaiki berdasarkan hasil analisis gap dan studi literatur yang dilakukan. Kemudian, perbaikan kerangka FMEA tersebut diimplementasikan kembali sebagai validasi empiris.

FMEA Tradisional berdasarkan hasil *action research* siklus pertama terbukti tidak konsisten. Hal ini dikarenakan hasil RPN tim pertama terdapat 3 risiko pada tingkatan *very high* sedangkan tim kedua terdapat 7 risiko pada tingkatan *very high*. Pada siklus *action research* 2 terbukti bahwa hasil pengukuran risiko dengan FMEA *improvement* lebih konsisten. Hasil RPN yang didapatkan oleh kedua tim adalah sama, sehingga dapat disimpulkan kelemahan FMEA dapat terminimalisir dengan menerapkan kerangka perbaikan FMEA *Improvement*.

Kata kunci: *FMEA, Konsistensi FMEA, Risiko TI*

(Halaman sengaja dikosongkan)

CONSISTENCY ANALYSIS OF INFORMATION *TECHNOLOGY* RISK RESULT BY FAILURE MODE EFFECT AND ANALYSIS (FMEA)

Student Name : Nina Fadilah Najwa
Student Identification Number : 05211650012003
Supervisor :Dr. Apol Pribadi S, S.T, M.T

ABSTRACT

Failure Mode and Effect Analysis (FMEA) was one of the methods in risk management that could be used in various fields such as manufacturing and service industries, profit and non profit organizations, private organizations, public, or governmental organizations. Some studies have criticized the FMEA method because of the limitation or weakness of FMEA usage, especially on the issue of consistency. If FMEA is used improperly or inconsistent results will result in loss to the organization. This was because, the priority of risk requires a greater cost at the highest risk of ranking. These risk ranking differences could occur errors in prevention or focus on handling. The purpose of this study was to contribute research by synthesizing the FMEA framework to minimize the issue of consistency and subjectivity in risk management.

This research used two cycles of action resereach (plan, act, observe, reflect). The first cycle in *action research* to test and prove the consistency of Traditional FMEA. The stages in the consistency analysis were to analyze IT risk by two different teams in the same case study. Differences in risk ratings made by both teams would be analyzed for gaps and proposed improvements. In the second *action research* cycle, the process was to implement the synthesized FMEA framework. Initial stages by performing an improved FMEA frame synthesis based on gap analysis results and literature studies conducted. Then, the improvement of the FMEA framework was re-implemented as empirical validation.

Traditional FMEA based on the results of the first action research cycle proved inconsistent. This was because the first team RPN had 3 risks at very high levels while the second team had 7 risks at very high levels. In the second action research cycle, it was proven that risk measurement result with FMEA improvement was more consistent. The RPN results obtained by both teams were similar, so it could be concluded that FMEA weakness could be minimized by applying the FMEA Improvement methodology.

Keywords: *FMEA, Konsistensi FMEA, Risiko TI*

(Halaman sengaja dikosongkan)

KATA PENGANTAR

Dengan memanjatkan puji syukur kehadirat Allah SWT, karena berkat rahmat dan karunia-nya, penulis dapat menyelesaikan tesis yang berjudulanalisis konsistensi hasil risiko teknologi informasi *failure mode effect and analysis* (FMEA). Tesis ini merupakan salah satu syarat kelulusan dari Program Pascasarjana dari Departemen Sistem Informasi, Fakultas Teknologi Informasi dan Komunikasi, Institut Teknologi Sepuluh Nopember Surabaya. Penulis menyadari dalam mengerjakan tesis ini telah banyak mendapat bimbingan, bantuan, dan dukungan dari berbagai pihak. Sehingga pada kesempatan ini, penulis mengucapkan terima kasih dan penghargaan serta ungkapan terima kasih yang sebesar-besarnya atas segala bantuan kepada :

1. Orangtua dan keluarga besar yang telah senantiasa mendukung penulis dan memotivasi hingga laporan ini terselesaikan.
2. Bapak Dr. Apol Pribadi Subriadi, S.T., MT selaku Dosen Pembimbing yang telah meluangkan waktu, tenaga, pikiran, serta memberikan ilmu, dukungan, dan kesabaran selama membimbing penulis dari awal hingga tesis ini selesai.
3. Bapak Tony Dwi Susanto, S.T., M.T., Ph.D dan Bapak Faizal Mahananto, S.Kom., M.Eng., Ph.D selaku Dosen Penguji yang telah bersedia menguji dan memberikan masukan untuk penelitian ini.
4. Ibu Dr.Okfalisa, S.T., M.Sc dan Bapak Eki Saputra S.Kom selaku praktisi TI dalam penelitian ini yang telah bersedia membantu peneliti dan meluangkan waktunya untuk penelitian ini. Kemudian, Bapak Aresto Yudo S.Kom, M.Sc, CGEIT, CISA selaku validator pakar dalam penelitian ini.
5. Bapak/Ibu yang ada pada Bidang Penyelenggaraan Haji dan Umrah Kantor Wilayah Kementerian Agama Provinsi Riau yang telah meluangkan waktu dan membantu peneliti dalam mengimplementasikan kerangka FMEA tradisional dan kerangka FMEA yang telah disintesis.
6. Seluruh Bapak dan Ibu dosen beserta staf karyawan di Departemen Sistem Informasi, Fakultas Teknologi Informasi dan Komunikasi, Institut Teknologi Sepuluh Nopember.

7. Seluruh teman-teman keluarga besar S2 SI, terkhusus untuk angkatan 2016-Genap yang telah menemani suka duka penulis selama menempuh pendidikan magister.
8. Semua pihak yang namanya tidak dapat disebutkan satu persatu.

Dalam penulisan laporan ini, penulis sangat menyadari bahwa masih terdapat kekurangan yang harus diperbaiki. Untuk itu penulis menerima kritik dan saran yang membangun dari semua pihak untuk kesempurnaan laporan ini dan agar dapat lebih baik di masa yang akan datang. Penulis mengharapkan semoga laporan ini dapat bermanfaat bagi kita semua. Penulis menyampaikan doa dan harapan semoga Allah SWT membalas semua kebaikan yang telah diberikan semua pihak yang terkait dalam penyusunan laporan ini dengan melimpahkan rahmat dan anugerah-Nya kepada kita semua.

Surabaya, 18 Juli 2018

Nina Fadilah Najwa

DAFTAR ISI

DAFTAR GAMBAR

(Halaman sengaja dikosongkan)

DAFTAR TABEL

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Manajemen risiko merupakan salah satu topik yang termasuk dalam ruang lingkup penelitian sistem informasi (Sidorova, Evangelopoulos, Valacich, & Ramakrishnan, 2008). Manajemen risiko merupakan penerapan sistematik dari manajemen strategis, prosedur, dan praktis untuk mengidentifikasi, menganalisa, melakukan kontrol, serta mengawasi proses risiko. Hal ini penting dilakukan untuk menjamin kualitas yang baik dan menurunkan risiko kegagalan sebuah produk ataupun jasa (Zhao & Bai, 2010). Organisasi dapat mengelola risiko umum yang terdapat dalam aktivitas rutin sehingga aktivitas lebih efektif dan memperoleh hasil yang lebih baik dengan biaya yang rendah (Kakvan, Mohyeddin, & Gharaee, 2014).

Terdapat banyak metode yang dapat digunakan untuk analisis risiko seperti yang terdapat pada ICH Q9 tentang manajemen risiko kualitas. Adapun metode tersebut adalah *Failure Modeand Effects Analysis* (FMEA), *Failure Mode, Effects and Criticality Analysis* (FMECA), *Fault Tree Analysis* (FTA), *Hazard Analysis and Critical Control Points* (HACCP), *Hazard Operability Analysis* (HAZOP), *Preliminary Hazard Analysis* (PHA) dan *Risk Ranking and Filtering* (van Leeuwen et al., 2009). FMEA adalah salah satu teknik yang penting dalam memanajemen risiko terkait hal-hal apa yang harus dipahami dan diutilisasi. FMEA dibangun berdasarkan kolaborasi lingkungan, termasuk didalamnya pegawai dan keseluruhan aspek dari aktivitas proses bisnis perusahaan (Gary Teng, Ho, Shumar, & Liu, 2006). FMEA menyediakan struktur dan bahasa yang umum sehingga dapat digunakan oleh tim dalam industri manufaktur dan jasa, organisasi profit dan non profit, organisasi *private*, publik, ataupun organisasi pemerintahan (McDermott, Mikulak, & Beauregard, 2009).

Penggunaan FMEA secara tepat terbukti dapat mengurangi siklus dari biaya garansi dan memakan biaya yang sedikit untuk melakukan pencegahan dibandingkan memperbaiki permasalahan yang sudah terjadi (Carlson, 2014).

Pengunaan FMEA dapat diterapkan pada bagian keamanan, keuangan, perancangan perangkat lunak, sistem atau teknologi informasi, pemasaran, sumber daya manusia, dan pembelian(McDermott et al., 2009). Khususnya, pada bagian sistem atau teknologi informasi membahas penggunaan FMEA untuk menentukan keamanan dari data-data yang sensitif. Pemilihan FMEA merupakan metode yang umum digunakan dan dapat didokumentasikan dengan baik (van Leeuwen et al., 2009).

Beberapa penelitian mengkritisi FMEA karena limitasi atau kelemahan dari penggunaan metode ini. Kelemahan terjadi terutama pada saat melakukan perhitungan RPN karena adanya unsur subjektifitas, nilai potensial RPN tidak berkelanjutan, terdapat nilai RPN yang duplikat, para praktis menyebutkan RPN tidak disarankan untuk digunakan (Carlson, 2014). Secara tradisional, FMEA hanya mempertimbangkan dampak dari satu kegagalan dari sebuah sistem, sehingga perlu dicermati strategi dalam pendefinisian risiko dan perhitungannya(Xiao, Huang, Li, He, & Jin, 2011). Sehingga, hasil dari analisis risiko dengan menggunakan FMEA terdapat isu konsistensi dan subjektifitas (Estorilio & Posso, 2010), (Barends, Oldenhof, Vredenbregt, & Nauta, 2012), (Oldenhof et al., 2011), (Gary Teng et al., 2006).

Permasalahan umum yang ada pada FMEA berdasarkan pengalaman (Gary Teng et al., 2006), bahwa kurangnya informasi yang rinci pada fungsi produk atau bagian, mode potensial kegagalan, potensi dampak dari kegagalan, potensi penyebab kegagalan, dan perancangan kontrol yang ada. Sehingga, dengan kurangnya informasi ini menyebabkan kesalahpahaman, kebingungan atau ketidakpastian dalam pendefinisian risiko. Permasalahan lainnya adalah integritas dokumen FMEA yang termasuk permasalahan tidak konsistennya peringkat pada *severity*, *occurrence*, dan *detection*, yang beberapa bagian dari laporan FMEA hilang, tidak adanya rekomendasi untuk risiko yang tinggi berdasarkan RPN, dan perubahan skala dari peringkat setelah melakukan koreksi.

Isu subjektif dalam melakukan prioritisasi risiko merupakan salah satu limitasi yang didapatkan berdasarkan literatur review yang telah dilakukan. Kegiatan prioritisasi dilakukan berdasarkan emosi manusia dan pikiran, sehingga terdapat keraguan dalam keakuratan konsep yang berasal dari parameter yang

digunakan. Tim FMEA akan sulit menentukan perbedaan opini yang terjadi dalam perhitungan, dan variabel yang dibutuhkan dalam menghitung angka risiko yang tidak sesuai dan meragukan (Kakvan et al., 2014). Kesalahan pendefinisian risiko bergantung pada pengalaman anggota tim dalam menganalisis kegagalan dan familiarnya sistem bagi anggota serta bias kognitif yang diketahui.

Subjektivitas terjadi ketika kurangnya data mengenai kejadian dan efek kegegalan yang diketahui (Banghart, 2014).Sehingga, subjektivitas menyebabkan hasil yang tidak konsisten dan memerlukan strategi dalam melakukan penilaian risiko. Kemudian, FMEA hanya membantu dalam mengidentifikasi kemungkinan proses yang gagal, tetapi tidak mengeliminasinya, sebagai tambahan perlu adanya usaha untuk membangun rencana aksi dan mengimplementasikannya(Jain, 2017). Sehingga,tidak hanya mampu menggunakan FMEA tetapi juga mengimplementasikan aksi perbaikan.

Setiap organisasi menginginkan pendukung dalam produk dan proses dari segi keamanan, bebas masalah selama menjalankan kegiatan bisnis. Terutama pada bidang Teknologi Informasi yang membutuhkan keamanan informasi yang merupakan aset kritis organisasi. Kemanan informasi memiliki aspek kerahasiaan (*confidentiality),* keutuhan (*integrity*) dan ketersediaan (*availability*)(Whitman & Mattord, 2012). Risiko terkait keamanan informasi juga beragam, seperti kehilangan data akibat virus ataupun penyalahgunaan data oleh orang yang tidak berwenang. Risiko-risiko keamanan informasi tersebut akan berdampak bagi organisasi baik secara finansial maupun non-finansial. Sehingga, jika organisasi tidak mengetahui risiko yang akan dihadapi maka organisasi tidak dapat melakukan tindakan pencegahan dan perlindungan yang efektif.

Ketika FMEA digunakan secara tepat, maka FMEA dapat mengantisipasi dan mencegah masalah, mengurangi biaya, mempersingkat waktu produksi, dan mencapai keamanan dan produk/jasa yang terpercaya (Carlson, 2014). Akan tetapi, jika FMEA digunakan secara tidak tepat ataupun terdapatnya hasil yang tidak konsisten, akan memberikan kerugian pada organisasi. Hal ini dikarenakan, prioritas risiko tertinggi membutuhkan biaya yang lebih besar pada risiko lainnya.Perbedaan peringkat risiko tersebut dapat terjadi kesalahan dalam pencegahan atau fokus penanganan. Akan tetapi, tidak selalu hasil risiko yang

tidak konsisten pada FMEA mengindikasikan kelemahan yang buruk pada prosedur analisis risiko. FMEA yang dilakukan oleh dua tim yang berbeda akan memberikan informasi yang bernilai yang tidak diidentifikasikan oleh tim lainnnya (Oldenhof et al., 2011). Perbedaan tersebut menimbulkan pendefinisian risiko baru yang sebelumnya tidak ada. Sehingga, masing-masing tim FMEA akan diberikan kebebasan dalam menggunakan pendekatan FMEA ini secara fleksibel untuk mendefinisikan risiko yang ditemukan.

Berdasarkan latar belakang yang telah dikemukakan tersebut, maka penelitian ini menganalisa konsistensi hasil risiko Teknologi Informasi dengan menggunakan FMEA dengan memberikan perbaikan kerangka FMEA yang telah diformulasikan. Implementasi kerangka FMEA dilakukan pada Kantor Wilayah Kementerian Agama Provinsi Riau sebagai validasi empiris.

1.2 Perumusan Masalah

Berdasarkan kesenjangan yang menjadi latar belakang penelitian, pertanyaan besar yang ingin dijawab melalui penelitian ini yaitu:

1. Bagaimana konsistensi hasil dari penggunaan FMEA?
2. Apakah variabel atau komponen yang cenderung tidak konsisten pada proses FMEA?
3. Apakah yang menyebabkan atau yang mempengaruhi konsistensi FMEA?
4. Bagaimana mensintesis kerangka FMEA untuk mengatasi konsistensi hasil risiko FMEA?
5. Bagaimana empiris dari hasil sintesis kerangka FMEA yang telah disintesis pada studi kasus?

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah untuk memberikan kontribusi penelitian dengan mensintesis kerangka FMEA untuk meminimalisir isu konsistensi dan subjektifitas dalam manajemen risiko.

1.4 Manfaat Penelitian

Manfaat dari penelitian ini mendapatkanacuan model dan hasilnya menjadi panduan bagi organisasi dalam melakukan analisis risiko dengan menggunakan kerangka kerja FMEA yang telah disintesiskan.

1.5 Kontribusi Penelitian

Adapun kontribusi yang akan dihasilkan pada penilitian ini adalah:

1. Memberikan kontribusi teori berupa kerangka FMEA yang disintesiskan dengan melihat limitasi dari FMEA serta memberikan strategi pada setiap tahapan guna meminimalisir isu konsistensi FMEA yang telah dipaparkan pada penelitian terdahulu. Penelitian ini memberikan kritisasi terhadap FMEA tradisional yang saat ini masih digunakan dalam ranah manajemen risiko, sehingga dengan melihat limitasi serta keunggulan FMEA dapat memberikan suatu perbaikan terhadap kerangka FMEA. Penelitian ini juga memberikan kontribusi dalam penggunaan FMEA dalam bidang Teknologi Informasi.
2. Memberikan kontribusi bagi tim FMEA dengan adanya panduan dari kerangka kerja FMEA yang telah disintesis. Kemudian, kritisasi FMEA bagi para akademisi sebagai area yang perlu banyak diteliti dari berbagai perspektif.

1.6 Batasan Penelitian

Agar dalam penulisan penelitian ini dapat terarah dan terfokuskan serta tidak melebar membahas permasalahan diluar pembahasan yang ada, penulis memberikan batasan masalah yaituFMEA yang diformulasikan dengan meningkatkan kinerja dari setiap langkah FMEA tradisional sehingga dapat digunakan dengan mudah oleh tim penilaian risiko dan mendapatkan hasil yang konsisten.Kerangka FMEA yang diuji hingga proses pemrioritasan RPN dari hasil pemberian nilai *severity, occurrence* dan *detection.* Kemudian, risiko yang dianalisis pada penelitian ini adalah risiko keamanan Teknologi Informasi.

1.7 Sistematika Penulisan

Sistematika penulisan laporan penelitian yang dilakukan adalah sebagai berikut :

Bab 1: Pendahuluan

Bab ini terdiri dari latar belakang dilakukannnya penelitian, perumusan masalah, tujuan, batasan penelitian, kontribusi penelitian dan sistematika penulisan.

Bab 2 : Kajian Pustaka

Bab ini berisi kajian terhadap teori dan penelitian-penelitian yang sudah ada sebelumnya. Kajian pustaka ini bertujuan untuk memperkuat dasar dan alasan dilakukan penelitian.

Bab 3 : Metodologi Penelitian

Bab ini membahas mengenai rancangan penelitian, lokasi dan tempat penelitian, dan juga tahapan-tahapan sistematis yang digunakan selama melakukan penelitian.

Bab 4 : Hasil Penelitian dan Pembahasan

Bab ini menjelasakan hasil dari penelitian serta pembahasan sesuai dengan tujuan penelitian dan rumusan permasalahan.

Bab 5 : Kesimpulan dan Saran

Bab ini berisi simpulan dan saran yang didapatkan dari analisis terhadap hasil penelitian.

BAB 2
KAJIAN PUSTAKA

2.1. Kajian Teori

Kajian teori adalah teori mengenai konsep FMEA yang digunakan dalam penyusunan tesis. Kajian yang dilakukan dalam penelitian ini harus mengacu pada beberapa teori yang tepat dan sejalan dengan kerangka penelitian yang akan dikembangkan terkait konsep FMEA dalam manajemen risiko TI.

2.1.1 Risiko

Risiko adalah dampak negatif dari pelaksanaan yang memiliki kerentanan, mengingat adanya probabilitas dan dampak terjadinya sebuah kejadian. Lebih lanjut, pengertian risiko adalah fungsi dari kemungkinan sumber ancaman yang menggunakan potensi kerentanan tertentu, dan dampak yang dihasilkan dari kejadian buruk pada organisasi (Stoneburner, Goguen, & Feringa, 2002). Risiko TI adalah risiko yang terkait dengan penggunaan TI secara intensif untuk mendukung dan memperbaiki proses bisnis dan bisnis secara keseluruhan.

Risiko TI juga berkaitan dengan ancaman dan bahaya karena pemakaian TI secara intensif yang mungin menyebabkan kerusakan yang tidak diinginkan atau tidak terduga, kesalahan penggunaan dan kerugian dalam keseluruhan model bisnis dan termasuk lingkungannya (Spremic & D, 2008). Adapun ancaman adalah potensi sumber ancaman tertentu untuk berhasil menyerang kerentanan tertentu. Kerentanan adalah kelemahan yang secara tidak sengaja dipicu atau sengaja dieksploitasi. Sumber ancaman tidak menimbulkan risiko bila tidak ada kerentanan (Stoneburner et al., 2002).

Pada umumnya, sumber ancaman berasal dari:

1. Ancaman alam/alami (banjir, gempa bumi, tornado, longsor, petir, dan kejadian alam lainnya).
2. Ancaman manusia (kejadian yang disebabkan oleh manusia, seperti tindakan yang tidak di sengaja (kesalahan memasukkan data) atau tindakan yang di sengaja (serangan berbasis jaringan, mengunggah perangkat lunak berbahaya, memiliki hak akses yang tidak sah ke informasi rahasia).

3. Ancaman lingkungan (kegagalan dalam jangka panjang, polusi, kimiawi, kebocoran cairan).

Organisasi dapat menganalisa tingkat pengurangan risiko yang dihasilkan oleh kontrol baru atau yang disempurnakan dalam hal kemungkinan atau dampak ancaman berkurang, dua parameter yang didefinisikan pada level mitigasi untuk misi organisasi. Berikut ini adalah kontrol yang dilakukan untuk mitigasi risiko:

1. Menghilangkan beberapa kerentanan sistem (kekurangan dan kelemahan), sehingga mengurangi jumlah kemungkinan sumber ancaman dan kerentanan.
2. Menambahkan kontrol yang ditargetkan untuk mengurangi kapasitas dan motivasi sumber ancaman.
3. Mengurangi besarnya dampak buruk (misalnya, membatasi tingkat kerentanan atau modifikasi sifat hubungan antara sistem TI dan misi organisasi).

2.1.2 Manajemen Risiko

Konsep dari manajemen risiko pertama kali dikenalkan oleh Doug Barlow di USA sekitar tahun 1950 dan di UK pada tahun 1969 (Simister, 2000). Manajemen risiko TI adalah proses yang dapat dilakukan oleh manajer IT untuk menyeimbangkan antara operasional dan biaya ekonomi untuk tindakan perlindungan dan mencapai keuntungan dalam kemampuan misi dengan melindungi sistem dan data TI yang mendukung tujuan organisasi. Sehingga, organisasi harus menentukan kemampuan keamanan yang harus dimiliki sistem TI mereka untuk memberikan tingkat dukungan misi yang diinginkan dalam menghadapi ancaman dunia nyata. Sebagian besar organisasi memiliki anggaran yang ketat untuk keamanan TI. Oleh karena itu, pengeluaran biaya untuk keamanan TI harus ditinjau secara menyeluruh seperti keputusan manajemen lainnya. Metodologi manajemen risiko terstruktur dengan baik, bila digunakan secara efektif, dapat membantu manajemen mengidentifikasi kontrol yang tepat untuk menyediakan kemampuan keamanan penting bagi misi organisasi (Stoneburner et al., 2002).

Menurut Gottfried (1989), tujuan dari manajemen risiko TI adalah untuk melindungi aset TI seperti data, perangkat keras, perangkat lunak, personal dan

fasilitas dari seluruh ancaman faktor ekternal (seperti: bencana alam) dan faktor internal (seperti: kesalahan teknis, sabotase, akses yang tidak terotorisasi)(Bandyopadhyay, Mykytyn, & Mykytyn, 2011). Kemudian, menurut Rainer et al (1991), tujuan lain manajemen risiko adalah untuk menghindari atau mengurangi kerugian dengan memilih dan menerapkan kombinasi terbaik dari tindakan (Bandyopadhyay et al., 2011). Sehingga, dengan adanya manajemen risiko dapat meminimalisir biaya yang akan dikeluarkan jika ternyata kejadian risiko tersebut benar terjadi.

Menurut *Risk Management standard* AS/NZS 4360 (1999) dalam (Ahmed, Kayis, & Amornsawadwatana, 2008), proses manajemen risiko merujuk kepada menutupi kelemahan dalam suatu metode yang digunakan dalam pembangunan produk melalui pendekatan yang terstruktur sehingga aksi mitigasi dapat diinisiasi untuk mencegah risiko, perpindahan risiko, menurunkan kemungkinan risiko ataupun mengurangi dampak risiko. Terdapat proses manajemen yang diusulkan oleh AS/NZS 4360 terkait proses manajemen risiko. Proses tersebut terdiri dari tujuh tahapan iterasi sub proses dari konteks risiko yaitu identifikasi risiko, analisis risiko, evaluasi risiko, komunikasi dan konsultasi risiko melalui *stakeholder*, mengawasi dan mengatur kejadian risiko.

Sedangkan menurut Alexandeer (1992), proses manajemen risiko terdiri dari 4 tahapan yaitu identifikasi risiko menggunakan berbagai macam teknik dengan mengisi *form* ancaman, menganalisis dengan mengukur frekuensi dan tingkat keparahan jika terjadinya ancaman yang memungkinkan, mengontrol dengan mengukur fisik dan melakukan pelatihan pegawai untuk mengurangi penerimaan ancaman dan konsekuensi keuangan, dan menghitung biaya risiko dengan merencanakan perkiraan kerugian jika risiko terjadi ataupun biaya penanganan dan penanggulangan. Proses dari manajemen risiko tersebut diasumsikan sebagai strategi yang penting dalam organisasi untuk merencanakan pengurangan risiko dari kejadian yang terjadi dan atau meminimalkan dampak konsekuensi dari kejadian tersebut (Alexander, 1992). Strategi manajemen risiko secara umum terdiri dari empat strategi yaitu pencegahan risiko (mengurangi kemungkinan), mitigasi dampak (mengurangi dampak), transfer (melimpahkan

risiko pada pihak ketiga sebagai perusahaan asuransi penjamin risiko), dan penerimaan risiko (Emblemsvag, 2010).

Manajemen risiko secara umum terdiri dari tiga proses seperti dijelaskan di bawah ini (Stoneburner et al., 2002):

1. Penilaian Risiko (Risk Assessment)

Organisasi menggunakan manajemen risiko untuk menentukan potensi dari ancaman dan risiko yang berhubungan dengan sistem TI. Hasil yang diperoleh dari proses penilaian risiko akan membantu dalam mengidentifikasi kontrol yang sesuai untuk menurunkan atau mengeliminasi risiko selama proses mitigasi dilakukan. Penentuan kejadian yang mungkin terjadi pada masa yang akan datang, ancaman untuk sebuah sistem TI harus dianalisis dalam kesenjangan dengan potensi kerentanan dan kontrol situasi untuk sistem TI. Dampak yang diperoleh dari seberapa besarnya bahaya yang diakibatkan oleh ancaman kerentanan. Mengidentifikasi risiko sistem TI memerlukan pemahaman yang tajam tentang lingkungan pemrosesan sistem. Orang yang melakukan penilaian risiko harus mengumpulkan informasi yang berkaitan dengan sistem, yang biasanya diklasifikasikan sebagai berikut:

a. Perangkat Keras
b. Perangkat lunak
c. Antarmuka sistem (internal dan eksternal koneksitas)
d. Data dan informasi
e. Orang yang mendukung dan menggunakan sistem TI
f. Tujuan sistem (proses yang ditampilkan oleh sistem TI)
g. Sistem dan data kritis (sistem yang bernilai atau penting bagi organisasi).
h. Sistem dan data sensitif.

Sebagai tambahan, informasi yang berhubungan dengan lingkungan operasional dari sistem TI dan datanya, tetapi tidak terbatas, termasuk sebagai berikut:

a. Kebutuhan fungsional dari sistem TI

b. Pengguna sistem (pengguna sistem yang menjadi pendukung teknikal dari sistem TI; pengguna aplikasi yang menggunakan sistem TI untuk keperluan fungsi bisnis).
c. Tata kelola kebijakan keamanan sistem (peraturan organisasi, kebutuhan federal, hukum, praktis industri)
d. Arsitektur keamanan sistem
e. Topologi jaringan terkini
f. Perlindungan penyimpanan informasi yang diamankan oleh sistem dan ketersediaan data, integritas data
g. Alir informasi sistem TI (*flowchart* dari antar muka sistem, masukan sistem dan keluaran sistem)
h. Kontrol teknis sistem TI (produk keamanan *built-in* atau add-on yang mendukung identifikasi dan otentikasi, kontrol akses *discretionary* atau *mandatory*, audit, perlindungan informasi residual, metode enkripsi).
i. Kontrol manajemen yang digunakan untuk sistem TI (aturan perilaku, perencanaan keamanan).
j. Kontrol operasional untuk sistem TI (keamanan personal, *backup*, kontinjensi, dan operasi pemulihan kembali; perbaikan sistem; penyimpanan *off-site*; pembuatan akun pengguna dan prosedur penghapusan; kontrol untuk pemisahan fungsi pengguna, seperti akses pengguna istimewa dan akses pengguna standar).
k. Lingkungan keamanan fisik sistem TI (keamanan fasilitas, kebijakan pusat data).
l. Keamanan lingkungan diterapkan untuk lingkungan pemrosesan sistem TI (kontrol untuk kelembaban, air, listrik, polusi, suhu, dan bahan kimia).

Untuk sistem TI operasional, data dikumpulkan mengenai sistem TI di lingkungan produksinya, termasuk data tentang konfigurasi sistem, konektivitas, dan prosedur dan praktik terdokumentasi dan tidak berdokumen. Oleh karena itu, deskripsi sistem dapat didasarkan pada keamanan yang diberikan oleh infrastruktur yang mendasarinya atau pada rencana keamanan masa depan untuk sistem TI.

2. Mitigasi Risiko (Risk Mitigation)

Mitigasi risiko merupakan proses kedua dari manajemen risiko, termasuk didalamnya proses prioritisasi, evaluasi, dan implementasi dari kontrol reduksi risiko yang sesuai dan direkomendasikan dari proses penilaian risiko. Dikarenakan mengeliminasi keseluruhan risiko merupakan hal yang tidak mungkin, maka manajemen senior dan fungsional serta bisnis manajer berkewajiban dalam menggunakan pendekatan yang memiliki biaya rendah dan mengimplementasikan kontrol yang paling sesuai untuk meminimalisir risiko yang diterima.

Mitigasi risiko dapat dicapai melalui salah satu opsi mitigasi risiko berikut ini:

a. Asumsi Risiko. Menerima risiko potensial dan terus mengoperasikan sistem TI atau menerapkan kontrol untuk menurunkan risiko ke tingkat yang dapat diterima.
b. Penghindaran Risiko. Untuk menghindari risiko dengan menghilangkan penyebab dan atau konsekuensi risiko misalnya, mengabaikan beberapa fungsi sistem atau mematikan sistem saat risiko diidentifikasi.
c. Batasan Risiko. Untuk membatasi risiko dengan menerapkan kontrol yang meminimalkan dampak buruk ancaman yang menggunakan kerentanan misalnya, penggunaan kontrol detektif pendukung, pencegahan.
d. Perencanaan Risiko. Mengelola risiko dengan mengembangkan rencana mitigasi risiko yang memprioritaskan, menerapkan, dan memelihara kontrol.
e. Penelitian dan Pengakuan. Untuk menurunkan risiko kerugian dengan mengakui kerentanan atau kelemahan dan meneliti kontrol untuk memperbaiki kerentanan.
f. Transfer Risiko. Untuk mentransfer risiko dengan menggunakan opsi lain untuk mengkompensasi kerugian, seperti membeli asuransi.

3. Evaluasi dan pengukuran (Evaluation and Assessment)

Pada sebagian organisasi, jaringan pada organisasi akan terus diperluas dan diperbarui, komponennya berubah, dan aplikasi perangkat lunaknya diganti atau diperbarui dengan versi yang lebih baru. Selain itu, perubahan personil akan

terjadi dan kebijakan keamanan cenderung berubah dari waktu ke waktu. Perubahan ini berarti bahwa risiko baru akan muncul dan risiko yang sebelumnya dikurangi mungkin kembali menjadi perhatian. Dengan demikian, proses manajemen risiko terus berlangsung dan terus berkembang. Bagian ini menekankan praktik dan kebutuhan yang baik untuk evaluasi dan penilaian risiko yang sedang berlangsung dan faktor-faktor yang akan menghasilkan program manajemen risiko yang berhasil.

2.1.3 Definisi Aset

Aset dalam perspektif keamanan Teknologi Informasi adalah merupakan segala sesuatu yang bernilai yang harus dilindungi dari hal-hal yang membahayakan. Adapun aset-aset tersebut adalah sebagai berikut (Firesmith, 2003):

1. Orang adalah manusia yang dirugikan (terkena penyakit, terluka, atau terbunuh) karena kecelakaan/kegagalan yang terjadi. Orang-orang ini dapat diklasifikasikan menjadi:
    a. Korban bagian utama adalah korban yang menjadi bagian dari sistem (contohnya adalah operator, manajer, personel pemeliharaan).
    b. Korban bagian kedua adalah korban yang berasal dari eksernal sistem tetapi sering melakukan interaksi dengan internal (contohnya pengguna dan pemasok)
    c. Korban bagian ketiga adalah korban yang merupakan masyarakat umum yang tidak sengaja berada pada lokasi kejadian dan tidak berinteraksi dengan sistem.
    d. Korban bagian keempat adalah korban yang merupakan generasi yang akan datang yang terkena dampak radiasi, zat kimiawi, patogen yang dihasilkan dari kecelakaan yang terjadi.
2. Properti adalah segala kepemilikan yang bernilai yang mungkin hancur atau rusak jika terjadi kecelakaan. Adapun yang dimaksudkan properti tersebut adalah:

a. Kepemilikan eksternal adalah personal, komersil, dan milik pemerintah yang berada di luar sistem. Contohnya adalah data, uang, dan properti fisik seperti gedung dan fasilitas.
b. Komponen sistem adalah properti yang berada dalam komponen sistem termasuk data, perangkat keras, dan komponen perangkat lunak.

3. Lingkungan adalah lingkungan fisik yang mungkin hancur atau rusak jika terjadinya kecelakaan/kegagalan. Sebagai contoh adalah hasil dari terjadinya kecelakaan yang dapat merusak lingkungan seperti radiasi, zat-zat yang berbahaya, dsb., yang dapat merugikan masyarakat banyak.

   Berikut ini adalah hal-hal yang berkaitan dengan aset untuk mengelola aset:

   a. Keselamatan (*safety*) adalah perlindungan yang dilakukan untuk orang, properti dan lingkungan dari kecelakaan.
   b. Keamanan (*security*) adalah perlindungan properti (data) dan layanan (contohnya penolakan layanan) dari kecelakaan/kegagalan walaupun juga harus melindungi orang (contohnya perlindungan fisik) dan berbagai macam properti (contohnya pencurian perangkat keras, sabotase fasilitas, integritas perangkat lunak, dll).
   c. Keberlangsungan (*survivability*) adalah batasan yang dibuat untuk melindungi layanan yang penting dari kecelakaan. Akan ada bebrapa sekumpulan layanan yang menjadi prioritas dan akan selalu berubah. Jadi, keselamatan dan keamanan dari berbagai aset dapat berdampak secara langsung pada kemampuan sistem untuk menyediakan layanan penting sehingga aspek keberlangsungan ini dilakukan sebagai misi utama.

Menurut(Alberts & Dorofee, 2002)aset informasi terbagi menjadi :

1. Informasi, dokumen (kertas atau elektronik) data atau kepemilikan intelektual yang digunakan untuk mencapai misi dari organisasi.
2. Sistem, sistem informasi yang memproses dan menyimpan informasi (sistem yang memiliki komponen informasi, *software, hardware,* dan *host, client,* ataupun *server*)
3. *Software,* aplikasi dan layanan perangkat lunak seperti sistem operasi, aplikasi basis data, aplikasi jaringan, dan sebagainya.

4. *Hardware*, perangkat teknologi informasi fisikal.
5. Orang, orang yang ada di dalam organisasi yang melakukan tugas ataupun proses dengan keahlian khusus, memiliki pengetahuan dan pengalaman yang sulit untuk digantikan.

2.1.4 Aspek Keamanan Informasi

Keamanan adalah kualitas atau keadaan yang aman, yang bebas dari bahaya. Organisasi yang sukses harus memiliki tingkat keamanan yang berlapis dalam setiap operasinya, seperti dijabarkan di bawah ini (Whitman & Mattord, 2012):

1. Keamanan fisik, untuk melindungi benda fisik, objek, atau area dari akses yang tidak sah dan penyalahgunaan.
2. Keamanan personel, untuk melindungi grup atau individu yang memiliki akses yang sah dalam organisasi dan dalam operasionalnya.
3. Keamanan operasi, untuk melindungi detil dari operaasi khusus atau aktivitas yang berkelanjutan.
4. Keamanan komunikasi, untuk melindungi komunikasi media, teknologi dan konten.
5. Keamanan jaringan informasi, utnuk melindungi aspek keamanan informasi (*Confidentiality, integrity, availability*) dari aset informasi, yang mana tersimpan, diproses, dan ditransmisikan. Hal ini dilakukan dengan pengaplikasian kebijakan, pelatihan dan kesadaran, dan teknologi.

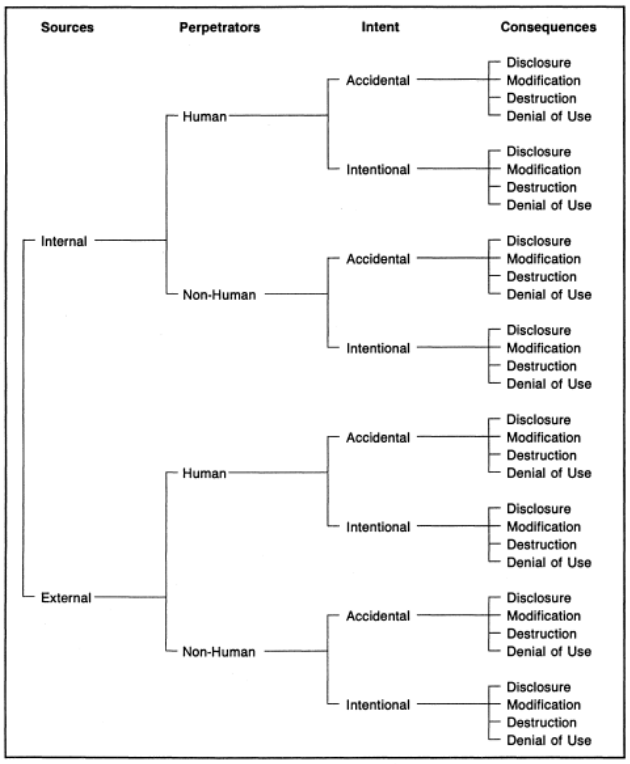
Adapun aspek keamanan informasi adalah sebagai berikut (Whitman & Mattord, 2012):

1. Kerahasiaan (*Confidentiality*) yang merupakan aspek menjamin kerahasiaan data ataupun informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang memiliki wewenang dan menjamin kerahasiaan data yang dikirim, diterima, dan disimpan.
2. Integritas (*Integrity*) merupakan aspek yang menjamin bahwa tidak adanya pengubahan data tanpa adanya izin oleh berwenang, serta menjaga keakuratan dan keutuhan informasi.

3. Ketersediaan (*Availability*) merupakan aspek yang menjamin bahwa data akan tersedia saat data tersebut diperlukan dan dapat diakses kapanpun dan dimanapun, serta memastikan pengguna yang berhak dapat menggunakan informasi dan perangkatnya.

2.1.5 Ancaman Keamanan Informasi

Ancaman adalah situasi yang meningkatkan kemungkinan dari satu atau lebih serangan. Ancaman ini berasal dari keberadaan dari satu atau lebih potensial penyerang dengan sekumpulan dari satu atau lebih kondisi sistem atau keadaan yang memberikan motivasi kepada penyerang (Firesmith, 2003). Sumber ancaman terdiri dari ancaman internal dan ancaman eksternal. Ancaman internal merupakan potensi kemungkinan terjadinya serangan yang bersumber dari internal organisasi. Sedangkan ancaman ekternal merupakan potensi kemungkinan terjadinya serangan yang berasal dari eksternal organisasi (Loch, Carr, & Warkentin, 1992). Secara terperinci dapat terlihat pada gambar di bawah ini:



Gambar 2.1. Ketegorisasi Ancaman Berdasarkan Sumber

Sumber : (Loch et al., 1992)

Berikut ini adalah kategori dari ancaman keamanan informasi(Whitman & Mattord, 2012):

Tabel 2.1. Kategori Ancaman

No	Kategori Ancaman	Contoh
1	Gangguan Kekayaan Intelektual	Pembajakan, pelanggaran hak cipta
2	Serangan perangkat lunak	Virus, *worms, macros,* penolakan layanan
3	Penyimpangan dalam kualitas layanan	ISP, *power*, atau masalah layanan WAN dari layanan penyedia
4	Pengintaian dan pelanggaran	Tidak sahnya akses dan atau pengumpulan data
5	Bencana Alam	Kebakaran, banjir, gempa bumi, petir
6	Kesalahan manusia atau kegagalan	Kecelakaan, kesalahan pegawai
7	Pemerasan informasi	*Blackmail*, pemberitahuan informasi rahasia
8	Hilang, tidak memadai atau tidak lengkap	Hilangnya akses terhadap sistem informasi karena kegagalan *disk drive* tanpa *backup* dan rencana pemulihan sesuai kebijakan dan perencanaan organisasi
9	Hilang, tidak memadai atau tidak lengkapnya kontrol	Jaringan terganggu karena tidak ada kontrol keamanan *firewall*.
10	Sabotase dan perusakan	Pemusnahan sistem atau informasi
11	Pencurian	Penyitaan peralatan atau informasi secara ilegal
12	Kegagalan atau error teknikal perangkat keras	Kegagalan peralatan
13	Kegagalan atau error teknikal perangkat lunak	*Bugs*, permasalahan kode, tidak diketahuinya celah (loopholes)
14	Keusangan teknologi	Teknologi kuno atau usang

Sumber: (Whitman & Mattord, 2012)

2.1.6 Failure Mode Effect and Analysis (FMEA)

Failure Mode and Effect Analysis (FMEA) telah digunakan sekitar lebih dari 40 tahun. FMEA secara formal pertama kali digunakan oleh industri penerbangan pada pertengahan tahun 1960an dan dikhususkan untuk isu-isu keselamatan atau keamanan. Jauh sebelum itu, FMEAs menjadi sebuah alat kunci untuk meningkatkan kemanan, terutama pada industri proses kimiawi. Tujuan dari keamanan dari FMEA ini adalah mengingat untuk mencegah ancaman keselamatan, dan insiden terjadinya kecelakaan. Ketika para teknikal selalu melakukan analisa proses dan produk untuk potensial kegagalan, pendekatan FMEA menstandarisasi proses tersebut dengan bahasa yang umum sehingga dapat digunakan dalam berbagai bidang organisasi. FMEA juga dapat digunakan oleh pegawai teknikal maupun pegawai non teknikal dari berbagai tingkatan (McDermott et al., 2009).

Failure Modes Effect Analysis (FMEA) menurut McCain (2006) adalah *tool* manajemen risiko yang digunakan untuk mengidentifikasi kegagalan yang akan terjadi dalam sebuah proses, produk ataupun layanan. Sebelum kegagalan tersebut terjadi, perlu dilakukan langkah-langkah proaktif yang dirancang dan diimplementasikan. Sebagian besar dari metode manajemen risiko adalah kualitatif dan deskriptif, sedangkan FMEA tergolong ke dalam semi-kuantitatif (Lai & Chin, 2014). Implementasi FMEA termasuk dalam membuat sebuah peringkat risiko yang disebut dengan *Risk Priority Number* (RPN) yang merupakan hasil dari menilai tingkat keparahan setiap potensi kegagalan pada pelanggan (*Severity*), kemungkinan terjadinya kegagalan (*Occurrence*) dan kemungkinan pendeteksian (*Detection*) sebelum pengaruh kegagalan mencapai pelanggan(Claxton & Campbell-Allen, 2017).

Pencengahan masalah proses dan produk sebelum terjadi adalah tujuan dari FMEA. Digunakan pada kedua proses yaitu perancangan dan manufaktur, secara substantif akan mengurangi biaya dengan mengidentifikasi produk dan proses meningkat lebih cepat dalam proses pembangunan ketika perubahan mudah dilakukan dan tidak mahal jika dibuat. Hasilnya adalah lebih terjaminnya proses karena mengurangi atau mengeliminasi aksi perbaikan sesudah terjadinya permasalahan dan krisis perubahan (McDermott et al., 2009).

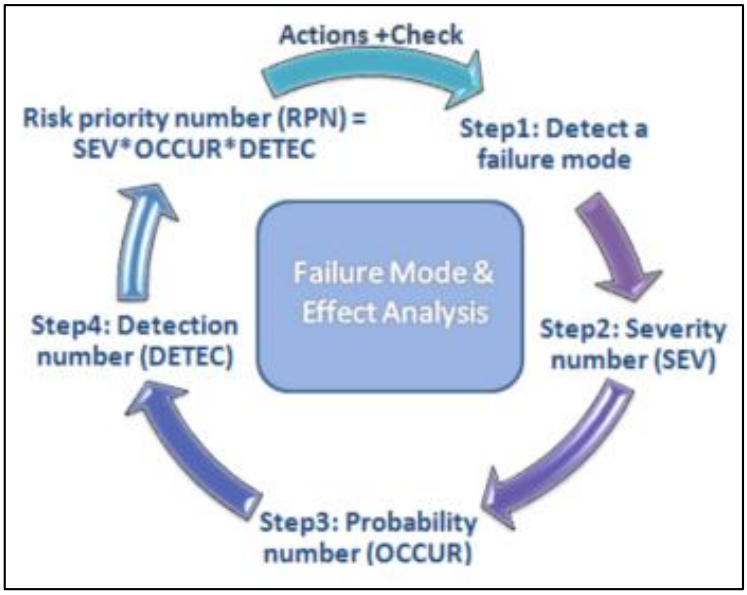
FMEA dilakukan pada perancangan produk ataupun tahapan pengembangan proses, hal ini dilakukan untuk mendapatkan keuntungan. Tim FMEA menentukan, dengan analisis mode kegagalan, dampak dari masing-masing kegagalan dan mengidentifikasi setiap poin kegagalan yang sangat penting. Selanjutnya akan dilakukan pemberian peringkat masing-masing kegagalan berdasarkan dampak kegagalan yang paling kritis dan mungkin terjadi (Lipol & Haq, 2011). Adapun hasil dari FMEA ini akan membantu para manajer dan teknisi untuk mengidentifikasi mode kegagalan, penyebabnya dan memperbaikinya (Sharma & Sharma, 2010).

FMEA memiliki beberapa tipe umum yaitu sistem FMEA, desain FMEA dan proses FMEA. Sistem FMEA dapat digunakan pada tingkatan analisis dari keseluruhan sistem, yang dibuat berdasarkan banyak sub sistem. Fokus dari tipe FMEA ini untuk keamanan sistem, integrasi sistem, antarmuka atau interaksi antara sub sistem dengan sistem lainnya, interaksi dengan lingkungan, interaksi manusia, layanan, dan berbagai isu lainnya yang dapat menyebabkan sistem tidak dapat bekerja bagaimana seharusnya. Desain FMEA berfokus pada perancangan produk, biasanya ditingkat subsistem atau komponen. Fokusnya adalah pada kekurangan yang berkaitan dengan desain, dengan memperhatikan pada peningkatan perancangan dan memastikan pengoperasian produk aman dan andal selama peralatan digunakan. Sedangkan, ruang lingkup Proses FMEA dapat mencakup operasi manufaktur dan perakitan, pengiriman, bagian masuk, pengangkutan bahan, penyimpanan, konveyor, perawatan alat, dan pelabelan.

Terdapat berbagai jenis FMEA yaitu seperti *Failure Mode Effects and Criticality Analysis* (FMECA) mirip dengan FMEA, dengan langkah tambahan dari analisis kritis yang lebih formal. Langkah tambahan ini biasanya membutuhkan data yang obyektif untuk mendukung perhitungan kekritisan. Dianjurkan bagi praktisi yang diminta untuk melakukan analisis FMECA untuk memahami dasar-dasar FMEA terlebih dahulu, dan kemudian mempelajari prosedur FMECA. Beberapa jenis FMEA lainnya termasuk Konsep FMEA, Pemeliharaan FMEA, Analisis Bahaya, *Software* FMEA.(Carlson, 2014)

2.1.6.1. Tahapan FMEA

FMEA memiliki beberapa tahapan, yang secara umum digambarkan pada gambar berikut ini:



Gambar 2.2 Tahapan FMEA

Pada gambar 2.2 terdapat beberapa tahapan dalam menggunakan FMEA, berikut penjelasan dari masing-masing tahapan (*Software*, 2016):

1. Identifikasi potensi kegagalan dan dampaknya
2. Menentukan tingkat keparahan (severity)
3. Menentukan nilai frekuensi sering terjadinya (occurence) kegagalan
4. Mendeteksi kegagalan (failure)
5. Melakukan kalkulasi *Risk Priority Number* (RPN)

Secara lebih rinci, tahapan umum tersebut lebih detail dijelaskan pada setiap tahapan berikut ini (McDermott et al., 2009):

1. Mengidentifikasi proses atau produk yang terkait.
2. Mengidentifikasi mode kegagalan (*failure modes*) dengan *brainstorming*.
3. Mengidentifikasi dampak dari mode kegagalan (*failure mode*)
4. Menentukan nilai keparahan (*severity*) dari kegagalan
5. Menentukan nilai frekuensi sering terjadinya (*occurence*) kegagalan.
6. Menentukan peringkat deteksi (*detection*) untuk masing-masing mode kegagalan dan atau dampaknya.

7. Melakukankalkulasi nilai RPN*(Risk Priority Number*) untuk setiap dampak.
8. Melakukan prioritisasi tindakan untuk mode kegagalan.
9. Melakukan tindakan untuk mengeliminasi atau mengurangi risiko tinggi dari mode kegagalan.
10. Melakukan kalkulasi RPN yang dihasilkan sebagai mode kegagalan yang dikurangi atau dieliminasi.

2.1.6.2. Penilaian Risiko dengan FMEA

Penilaian risiko dengan FMEA dengan memberikan nilai pada *severity*, *occurrence* dan *detection.* Berikut ini akan dijelaskan lebih lanjut mengenai ketiga komponen tersebut.

1. Penilaian tingkat keparahan (*severity*)

Nilai keparahan adalah nomor peringkat yang terkait dengan efek paling serius untuk mode kegagalan yang diberikan, berdasarkan pada kriteria dari skala keparahan(Carlson, 2014).Ini adalah peringkat relatif di dalam lingkup FMEA spesifik yang ditentukan tanpa memperhatikan kemungkinan terjadinya atau deteksi. Berikut ini adalah skala keparahan(Stamatis, 2003):

Tabel 2.2. Nilai Tingkat Keparahan

Dampak	Peringkat	Kriteria
Tidak Ada Akibat	1	Tidak ada dampak.
Akibat Sangat Ringan	2	Tidak terganggu. Sangat sedikit berpengaruh pada kinerja sistem.
Akibat Ringan	3	Sedikit terganggu tanpa kehilangan sesuatu.Penurunan kinerja sistem.
Akibat Minor	4	Penurunan kinerja sistem secara signifikan (Policy)
Akibat Moderat	5	Tidak dapat dioperasikan tanpa kerugian (Prosedur)
Akibat Signifikan	6	Tidak dapat dioperasikan dengan kerugian kecil (Proses)
Akibat Major	7	Tidak dapat dioperasikan dengan

		kerugian atau kerusakan peralatan
Akibat Ekstrim	8	Tidak dapat dioperasikan dengan kegagalan yang merusak tanpa mengorbankan keamanan.
Akibat Serius	9	Potensial kegagalan atau risiko mempengaruhi keamanan sistem dengan peringatan
Akibat Berbahaya	10	Potensial kegagalan atau risiko mempengaruhi keamanan sistem tanpa peringatan

Sumber : (Stamatis, 2003)

2. Penilaian nilai deteksi atau penyebab (*Detection*)

Sebuah penyebab adalah alasan spesifik untuk kesalahan yang biasanya ditemukan dengan menanyakan "kenapa" sehingga akar penyebab dapat ditentukan (Carlson, 2014). Berikut ini adalah skala nilai deteksi:

Tabel 2.3. Nilai Deteksi

Deteksi	Peringkat	Kriteria Metode Deteksi
Hampir Pasti	1	Hampir pasti dapat mendeteksi dengan waktu yang cukup untuk melaksanakan rencana kontingensi
Sangat Tinggi	2	Sangat tinggi dapat dideteksi dengan kontrol yang ada saat ini. Semua produk secara otomatis diperiksa.
Tinggi	3	Memiliki kemungkinan tinggi untuk dapat mendeteksi kegagalan
Cukup Tinggi	4	Memiliki kemungkinan cukup tinggi untuk dapat mendeteksi kegagalan
Sedang	5	Memiliki tingkat efektifitas yang rata-rata

Rendah	6	Memiliki tingkat efektifitas yang rendah
Sangat Rendah	7	Tidak handal dalam mendeteksi tepat waktu
Kecil	8	Tidak terbukti untuk mendeteksi tepat waktu
Sangat Kecil	9	Tidak mampu memberikan cukup waktu untuk melaksanakan rencana kontingensi
Hampir tidak mungkin	10	Kekurangan tidak dapat di deteksi penyebabnya. Tidak adanya metode deteksi.

Sumber : (Stamatis, 2003)

3. Penilaian nilai kemungkinan (*occurrence*)

Kemungkinan adalah sejumlah peringkat yang berhubungan dengan kemungkinan terjadinya mode kesalahan dan juga akan berhubungan dengan penyebab yang akan di analisa(Carlson, 2014). Berikut ini adalah peringkat nilai kemungkinan:

Tabel 2.4. Nilai Kemungkinan

Kemungkinan Kegagalan	**Peringkat**	**Kriteria**
Almost Never: Kegagalan hampir/tidak pernah terjadi	1	Satu kali dalam 6 - 50 tahun
Remote: Kegagalan terjadi relative kecil dan sangat jarang	2	Satu kali dalam 3 - 6 tahun
Very Slight: Kegagalan terjadi relatif kecil	3	Satu kali dalam 1-3 tahun
Slight : Kegagalan jarang terjadi	4	Satu kali dalam setahun
Low : Kegagalan terjadi sesekali waktu	5	Satu kali setiap 6 bulan

Medium: Kegagalan terjadi saat waktu tertentu	6	Satu kali setiap 3 bulan
Moderatly High : Kegagalan sering terjadi	7	Satu kali dalam sebulan
High: Kegagalan terjadi berulang kali	8	Satu kali dalam seminggu
Very High: Kegagalan selalu terjadi	9	Satu kali setiap 3-4 hari
Almost Certain: Kegagalan hampir/tidak dapat dihindari	10	Lebih dari satu kali tiap harinya

Sumber : (Stamatis, 2003)

Setelah penentuan nilai dari masing-masing *severity, occurrence* dan *detection*, maka selanjutnya dilakukan kalkulasi untuk pemrioritasan risiko dengan rumus RPN. Rumus RPN dihitung dengan mengalikan tingkat keparahannya dan tingkat terjadinya dan dikalikan dengan tingkat pendeteksian(McDermott et al., 2009). Jumlah total RPN harus dihitung dengan menambahkan semua nilai prioritas risiko. Nilai ini saja tidak ada artinya karena masing-masing FMEA memiliki jumlah mode kegagalan dan efek yang berbeda. Namun, bisa berfungsi sebagai mengukur untuk membandingkan RPN total revisi setelah tindakan yang direkomendasikan dilakukan telah dibentuk. Adapun rumus RPN tersebut adalah:

Risk Priority Number (RPN) = Severity x Occurence x Detection

Dari hasil yang didapatkan, maka penentuan level risiko didapatkan berdasarkan skala level risiko sebagai berikut:

Tabel 2.5 Nilai level risiko

Level Risiko	Skala Nilai RPN
Very High	> 200
High	< 200
Medium	< 120
Low	< 80
Very Low	< 20

Nilai RPN digunakan untuk menentukan komponen yang menjadi prioritas pertama untuk ditangani oleh perusahaan. Meskipun demikian, besarnya nilai RPN suatu komponen kritis, belum tentumenjadi prioritas pertama.

2.1.7. Pendekatan Kualitatif

Menurut Denzin & Lincoln (2011) dalam (Creswell, 2015), penelitian kualitiatif adalah suatu aktivitas yang berlokasi yang menempatkan penelitinya di dunia. Penelitian kualitatif terdiri dari serangkaian praktik penafsiran material yang membuat dunia menjadi terlihat. Praktik-praktik ini mentransformasikan dunia. Mereka mengubah dunia menjadi serangkaian representasi, yang mencakup berbagai catatan lapangan, wawancara, percakapan, foto, rekaman dan catatan pribadi. Dalam hal ini, penelitian kualitatif melibatkan suatu pendekatan penafsiran yang naturalistik terhadap dunia. Hal ini berarti bahwa para peneliti kualitatif mempelajari benda-benda di lingkungan alamiahnya, berusaha untuk memaknai atau menafsirkan fenomena dalam sudut pandang makna-makna yang diberikan oleh masyarakat kepada mereka.

Penelitian kualitatif dimulai dengan asumsi dan penggunaan kerangka penafsiran ataupun teoritis yang membentuk atau mempengaruhi studi tentang permasalahan riset yang terkait dengan makna yang dikenakan oleh individu atau kelompok pada suatu permasalahan sosial atau manusia. Untuk mempelajari masalah ini, para peneliti kualitatif menggunakan pendekatan kualitatif mutakhir dalam penelitian, pengumpulan data dalam lingkungan alamiah yang peka terhadap masyarakat dan tempat penelitian, dan analisis data yang bersifat induktif maupun deduktif dan pembentukan berbagai pola atau tema. Laporan

atau presentasi tertulis akhir mencakup berbagai suara dari para partisipan, refleksivitas dari peneliti, deskripsi dan interpretasi tentang masalah penelitian, dan kontribusinya pada literatur atau seruan bagi perubahan. (Creswell, 2015)

Lebih detail, ciri-ciri penelitian kualitatif adalah sebagai berikut(Creswell, 2015):

1. Lingkungan alamiah. Para peneliti kualitatif mengumpulkan informasi dengan berbicara secara langsung dengan masyarakat dan menyaksikan mereka berprilaku dan bertindak dalam lingkungan mereka. Para peneliti juga melakukan interaksi secara langsung pada objek penelitian.
2. Peneliti sebagai instrumen penting. Para peneliti menggunakan sebuah instrumen, tetapi merupakan instrumen yag dirancang oleh peneliti dengan menggunakan pertanyaan yang sifatnya terbuka. Para peneliti tidak cenderung menggunakan atau mengandalkan berbagai kuisioner atau instrumen yang dikembangkan oleh peneliti lain.
3. Beragam metode. Para peneliti biasanya menggunakan beragam metode bentuk data, misalnya wawancara, pengamatan, dan dokumen, daripada bersandar pada suatu sumber data tunggal.
4. Pemikiran yang kompleks melalui logika induktif dan deduktif. Para peneliti kualitatif membangun berbagai pola, kategori, dan tema mereka secara *"bottom up*", dengan mengorganisasikan data secara induktif menjadi satuan-satuan informasi yang semakin abstrak.
5. Pemaknaan partisipan. Sepanjang proses penelitian kualitatif, para peneliti menjaga fokusnya pada bagaimana mempelajari pemaknaan dari partisipan terhadap permasalahan atau isu tertentu, bukan pemaknaan yang dibawa oleh para peneliti ke dalam riset tersebut atau yang dibawa oleh para penulis lain.
6. Desain baru dan dinamis. Proses penelitian kualitatif selalu bersifat baru dan dinamis. Hal ini berarti bahwa perencaan awal dari riset tidak dapat ditetapkan secara pasti, dan bahwa semua tahap dari proses tersebut dapat sewaktu-waktu berubah atau bergeser setelah peneliti memasuki lapangan dan mulai mengumpulkan data.

7. Refleksivitas. Para peneliti menyampaikan (yaitu, dibagian metode, di bagian pengantar, atau di tempat lain dalam laporan penelitian) latar belakang mereka (misalnya, pengalaman kerja, pengalaman kebudayaan, sejarah, dan sebagainya), dan menjelaskan bagaimana semua ini mewarnai dan mempengaruhi penafsiran mereka terhadap informasi penelitian.
8. Pengembangan holistik. Para peneliti kualitatif mencoba mengembangkan gammbaran lengkap tentang permasalahan dalam studi.

Terdapat lima jenis pendekatan kualitatif, berikut ini adalah kelima pendekatan kualitatif (Creswell, 2015):

Tabel 2.6. Tipe pendekatan kualitatif

Tipe Pendekatan	Definisi	Ciri-ciri
Riset Naratif	Fokus pada narasi, cerita, atau deskripsi tentang serangkaian peristiwa terkait dengan pengalaman manusia.	1. Mengeksplorasi kehidupan seseorang individu 2. Butuh untuk menuturkan cerita tentang pengalaman individu 3. Mengambil dari humaniora. 4. Mempelajari satu atau lebih individu 5. Wawancara dan dokumen 6. Menganalisis data untuk cerita-cerita 7. Mengembangkan narasi cerita tentang kehidupan individu
Fenomenologi	Mencari "esensi: makna dari suatu fenomena yang dialami oleh beberapa individu.	1. Memahami esensi dari pengalaman 2. Butuh untuk mendeskripsikan esensi dari fenomena 3. Mengambil dari filsafat, psikologi, dan pendidikan 4. Mempelajari beberapa individu yang telah mengalami

		fenomena yang sama 5. Menggunakan wawancara dengan individu, meskipun dokumen, pengamayan dan kesenian mungkin juga dipertimbangkan 6. Menganalisis data untuk pernyataan-pernyataan penting, satuan-satuan makna, deskripsi tekstual dan struktural, dan deskripsi tentang esensi. 7. Mendeskripsikan esensi dari pengalaman.
Grounded Theory	Analisis abstrak terhadap suatu fenomena, dengan harapan dapat menciptakan teori tertentu yang dapat menjelaskan fenomena tersebut secara spesifik.	1. Mengembangkan *grounded theory* yang didasarkan pada data dari lapangan 2. Mendasarkan teori pada pandangan dari partisipan 3. Mengambil dari sosiologi 4. Mempelajari proses, aksi atau interaksi yang melibatkan banyak individu 5. Menggunakan terutama wawancara 6. Menganalisis data melalui *coding* terbuka, *coding* aksial, dan *coding* selektif. 7. Menyusun teori yang diilustrasikan dalam bagan/gambar
Etnografi	Suatu kelompok	1. Mendeskripsikan dan

	kebudayaan tertentu berdasarkan terutama pada pengamatan dan kehadiran peneliti di lapangan dalam waktu yang lama.	menafsirkan kelompok berkebudayaan sama 2. Mendeskripsikan dan menafsirkan pola kebudayaan yang sama dari kelompok 3. Mengambil antropologi dan sosiologi 4. Mempelajari kelompok yang memiliki kebudayaan sama 5. Menggunakan terutama pengamatan dan wawancara, tetapi mungkin juga mengumpulkan sumber lain selama waktu yang panjang di lapangan 6. Menaganalisis data melalui deskripsi tentang kelompok berkebudayaan sama dan tema-tema tentang kelompok tersebut. 7. Mendeskripsikan bagaimana kelompok berkebudayaan sama berjalan
Studi Kasus	Menelaah studi kasus tertentu dalam konteks atau *setting* kehidupan nyata kontemporer.	1. Mengembangkan deskripsi dan analisis mendalam tentang kasus atau beragam kasus (kasus majemuk) 2. Menyediakan pemahaman mendalam tentang kasus atau berbagai kasus 3. Mengambil dari psikologi

		hukum, sains dan politik, dan kedokteran 4. Mempelajari peristiwa, program, aktivitas, atau lebih dari satu individu 5. Menggunakan beragam sumber, seperti wawancara, pengamatan, dokumen, dan artefak 6. Menganalisis data melalui deskripsi tentang kasus dan tema dari kasus dan juga tema lintas kasus 7. Mengembangkan analisis detail tentang satu atau lebih kasus.

Sumber : (Creswell, 2015)

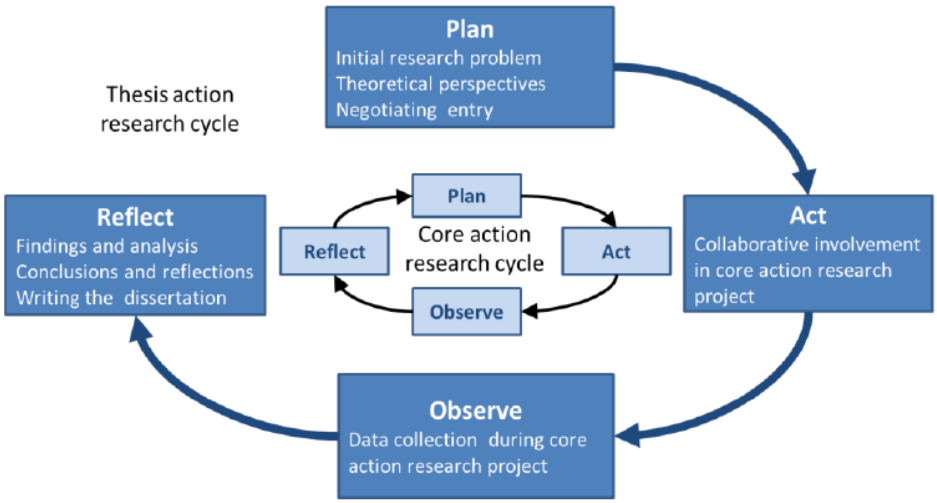
2.1.8 Analisis Kesenjangan (GAP Analysis)

Analisis gap dapat didefinisikan dengan penentuan perbedaan diantara pengetahuan atau praktik terkini (yang sedang dilakukan) dan dengan bukti dari *best practice* (apa yang harus dilakukan)(Janneti, 2012). Kesenjangan dapat terjadi dalam ruang lingkup pengetahuan, keterampilan ataupun praktis.Analisis kesenjangan menjadi salah satu teknik yang dapat membantu dalam mengidentifikasi keadaan yang saat ini dengan keadaan yang ingin dicapai dengan melengkapi kesenjangan tersebut. Kesenjangan dapat dilengkapi dengan solusi dari perbedaan yang ada agar dapat memenuhi keadaan yang dibutuhkan atau yang dituju.

2.1.9 *Action research*

Action research merupakan kerjasama kolaboratif antara peneliti dan kelompok dalam suatu organisasi atau masyarakat yang berpartisipasi dalam proses *action research.* Penelitian dilakukan dengan siklus perencanaan (*plan*), tindakan (*act*), pengamatan (*observe*) dan refleksi (*reflection*), di mana fase

refleksi membuka siklus lainnya untuk melakukan perbaikan (Rose, Spinks, & Canhoto, 2015). Berikut ini adalah siklus dari *action research*:



Gambar 2.3. Siklus *Action research*

Sumber :(Rose et al., 2015)

Penjelasan dari setiap proses adalah sebagai berikut:

1. *Plan.* Pada tahapan ini menciptakan rencana aksi yang akan mencapai tujuan yang telah disepakati. Rencana tersebut dapat mencakup perubahan dalam tiga 'register': bagaimana bahasa yang digunakan, kegiatan dan praktik apa yang akan dilakukan, dan bagaimana hubungan sosial dan struktur organisasi.
2. *Act.* Pada tahapan ini mengimplementasikan rencana dan juga menyadari perlunya fleksibilitas dan penilaian. Meski begitu, terkadang perlu untuk kembali ke tahap perencanaan jika tindakan yang diajukan tidak dapat dilaksanakan.
3. *Observe.*Tindakan harus disertai dengan pemantauan atau pengamatan terhadap hasilnya. Berbagai metode pengumpulan data dapat digunakan seperti dokumen, wawancara, catatan harian, kuisioner maupun observasi.
4. *Reflect.* Pada tahapan ini peneliti dan kelompok kolaborasi menganalisa, mensintesis, menginterpretasikan, menjelaskan dan menyimpulkan tentang apa yang telah dicapai. Pada tahapan ini juga memberikan perbaikan jika

adanya ketidaksesuaian. Siklus *action research* akan berakhir tergantung pada hasil yang ingin dicapai.

2.2. Penelitian Terdahulu

2.2.1 Ulasan Penelitian Terdahulu

Tidak seperti metode peningkatan kualitas lainnya, FMEA tidak menyediakan perhitungan statistik yang rumit. Akan tetapi, FMEA dapat menghasilkan penghematan yang signifikan bagi perusahaan bersamaan dengan penurunan potensi biaya yang mahal dari sebuah proses ataupun produk yang ternyata tidak sesuai dengan yang dijanjikan ataupun yang diharapkan. FMEA membutuhkan waktu dan sumber daya manusia Oleh karena itu, FMEA berdasarkan tim, sehingga dibutuhkan beberapa orang dalam prosesnya. Pondasi dari FMEA adalah anggota tim dan hasil masukan dari proses FMEA dan perlu adanya estimasi waktu dan pembagian tugas yang jelas (McDermott et al., 2009). Dari *paper* yang diperoleh, berikut ini akan dilakukan pengulasan *paper* sebanyak 31 paper berdasarkan kualitas isi. Pembuatan kriteria pengukuran kualitas *paper* dilakukan untuk memenuhi pertanyaan penelitian yang telah dirumuskan sebelumnya.

1. Bagaimana alur pikir (latar belakang, dasar teori, hal yang dikembangkan) dalam paper yang dibahas?
2. Apa kata kunci yang digunakan dalam paper yang dibahas?
3. Bagaimana solusi ataupun problem yang dikemukakan pada paper yang dibahas?
4. Bagaimana hasil temuan (teori dibantah atau tidak dan keterkaitan penelitian terdahulu) pada paper yang dibahas?
5. Apa keterbatasan dan peluang penelitian selanjutnya pada paper yang dibahas?
6. Apa rekomendasi yang ditawarkan paper yang dibahas baik teoritis maupun praktis?

Berikut ini adalah hasil dari penilaian kualitas isi berdasarkan enam pertanyaan tersebut.

Tabel 2.7. Ulasan berdasarkan kualitas isi

Penulis & Tahun	Alur Pikir	Kata Kunci	Masalah /solusi	Hasil	Limitasi/*future Research*	Rekomendasi
(Banghart, 2014)	Memberikan review dan saran perbaikan permasalahan yang ada pada FMEA dan berfokus pada potensial error pada perankingan. Membuat matriks HRI yang menurunkan bias dan lebih akurat hasil resiko yang didapat.	*human error and bias, data concern*	*Human error and bias* dan *data concern* mempengaruhi ketidakakuratan dari proses FMEA.	menerapkan *confidence interval* untuk kualifikasi resiko menambah pandangan baru terkait hasil model kegagalan di dalam suatu pembuatan keputusan.	metodologi untuk bagian lain dari analisis FMEA	Teoritis: matriks HRI yang menurunkan bias dan lebih akuratnya hasil resiko. Praktis: para teknikal
(Oldenhof et al., 2011)	Mengkritisi konsistensi FMEA dengan melakukan perbandingan hasil yang diperoleh oleh 2 tim yang berbeda. Kemudan, mengetahui letak perbedaan.	FMEA	Hasil yang tidak konsisten	FMEA selalu dilakukan di bawah pengawasan fasilitator FMEA berpengalaman dan tim paling sedikit dua anggota dengan kompetensi dalam metode analisis yang akan divalidasi. FMEA dari Kedua tim berisi informasi berharga yang tidak diidentifikasi oleh tim lain.	Perbaikan kerangka FMEA	Teoritis: kontribusi tentang kritisasi konsistensi hasil FMEA Praktis: bagi para manajer, dan tim pengukuran resiko
(Barends et al., 2012)	Konsistensi FMEA pada tahapan penilaian dengan RPN. Sehingga peneliti melakukan modifikasi FMEA dengan mensintesis juga FMECA yang terdapat *probabilty of occurrence*. Kemudian membandingkan hasil dari penilaian resiko FMEA tradisional dengan FMEA yang telah	*Traditional FMEA before & after improvement, Probabilistic FMEA before & after improvement*	modifikasi yang dilakukan dapat meningkatkan kekonsistensian hasil penilaian resiko.	Modifikasi peningkatan dilakukan pada tidak hanya RPN, tetapi juga kategori skor dari tingkat keparahan dan estimasi frekuensi yang tidak terdeteksi mode kegagalan. Kemudian,	Adanya subjektifitas sehingga memerlukan beberapa pengalaman tambahan dan Pelatihan tim FMEA.	modifikasi probabilistik FMEA untuk dapat digunakan oleh para medical dalam melakukan penilaian risiko.

	dikembangkan.			pendeteksian dapat dilakukan setiap tahunnya.		
(Sankar & Prabhu, 2001)	Kekurangan FMEA dieliminasi dengan teknik yang dikembangkan dari prioritasi resiko berdasarkan RPN konvensional. Sebuah skala baru didefinisikan dari kombinasi *severity, occurrence,* dan *detection,* yang disebut dengan *Risk Priority ranks* (RPRs).	*Severity, Occurrence, dan Detection*	Teknik yang baru untuk mengatasi limitasi dari RPN yang tradisional	Model kegagalan memiliki nilai RPR yang tinggi diasumsikan dapat lebih penting dan memberikan prioritas yang tinggi daripada memiliki nilai RPR yang rendah.	Perbaikan pada setiap peringkat yang tinggi dapat dilakukan. Memperhatikan risiko yang peringkat rendah untuk dilakukan revisi kembali.	Perbaikan kekurangan dari RPN pada FMEA. Dan kontribusi praktis adalah untuk Tim pengukur resiko pada sebuah perusahaan/instansi.
(Murphy, Heaney, & Perera, 2011)	Mempresentasikan sebuah metodologi untuk mengekstrasi batasan inovasi dari pembangunan project melalui manajemen stakeholder kompetensi dan FMEA.	Inovasi dan FMEA	metodologi untuk mendapatkan tingkatan yang besar dari pengadopsian inovasi terbaru dan meningkatkan rasa percaya diantara *stakeholder.*	Paper ini membuktikan bahwa tidak adanya batasan proyek yang mensyaratkan manajemen untuk melakukan inovasi, tetapi kegagalan pada kompetensi stakeholder.	Keuntungan dari FMEA sebagai alat ukur resiko pada penelitian pembangunan inovasi dan menggeneraskan kepada database yang dapat digunakan sebagai acuan kerangka kerja untuk penelitian selanjutnya.	Teoritis: Pendekatan pada stakeholder dimana keberhasilan inovasi karena pengimplementasian dilakukan pada kompetensi *stakeholder* yang benar pada tahapan yang benar. Praktis: untuk para designer proyek dalam perusahaan
(Chemweno, Pintelon, Van Horenbeek, & Muchiri, 2015)	Organisasi tersebut dapat memilih teknik pengukuran resiko yang bervariasi tergantung pada faktor-faktor yaitu tipe dari teknik, domain aplikasi, dan jumlah penilaian yang diberikan. Masih jarang teknik yang digeneralisasikan.	*Selection criteria, risk assessment techniqu e, risk assessment prosess, maintenance decision support, policy*	melakukan review (FMEA, FTA, BN) pemilihan teknik pada domain pemeliharaan aset.	Metodologi seleksi membentuk dasar untuk membandingkan kompetensi intrinsik perusahaan pada umumnya terhadap memprioritaskan kompetensi.	mengembangkan metodologi alternatif yang lebih kompleks. Penambahan teknik lainnya untuk mendokumentasikan pengetahuan tacit untuk diaplikasikan pada	Teoritis: kontribusi kerangka metodologi ANP dalam pemilhan teknik pengukuran resiko Praktis: Salah satu alat pendukung keputusan untuk praktisi pemelihara.

					teknik pengukuran resiko yang berbeda.	
(van Leeuwen et al., 2009)	prosedur *Near Infrared* (NIR) yang digunakan untuk menyaring obat-obatan pada FMEA, termasuk risiko teknis, faktor risiko kegagalan manusia.	NIR, FMEA, RPN	NIR dalam FMEA	FMEA dapat meningkatkan metode NIR, dan pengaruh faktor manusia.	RPN masih subjektif.	Teoritis: validasi analitik dengan FMEA Praktis: Farmasi
(Sellappan, Nagarajan, & Palanikumar, 2015)	Memberikan pendekatan baru untuk mengevaluasi RPNs dan mode kegagalan untuk meningkatkan teknik FMEA tradisional. Metode tersebut diuji pada studi kasus. Dan mengkonfirmasi metode yang diusulkan dengan analisis faktor secara statistik.	RPN	Metode yang diusulkan dapat lebih baik meningkatkan keakuratan hasil pengukuran risiko (RPN).	Hasil analisis statistik adalah mendukung kegunaan dari metodologi yang diusulkan dalam kondisi: tim FMEA tidak setuju dengan skala peringkat indeks S, O dan D. Rata-rata RPN identik untuk lebih dari satu mode kegagalan, dan semua indeks sama-sama penting.	Perlu adanya pengujian metodologi pada kasus berbeda dan pengembangan dari tahapan FMEA lainnya.	Teoritis: kontribusi pendekatan yang baru untuk prioritisasi RPN dengan analisis studi kasus. Praktis: Untuk tim FMEA dalam melakukan prioritisasi RPN
(Gary Teng et al., 2006)	Menarik perhatian penelitian pada implementasi dalam lingkungan kolaboratif, isu yang terjadi dalam proses implementasi (permasalahan dan limitasi dari FMEA) dan sebuah *tool* yang dapat digunakan pada seluruh bagian lingkungan kolaboratif untuk FMEA proses.	FMEA *Process*	Bagaimana mengimplementasikan prosedur FMEA dalam rantai pasok, dan masalah umum yang terjadi dalam pengimplementasian dibawah lingkungan kolaboratif.	Menyediakan contoh dari hasil yang tidak konsisten dalam peringkat S, D, dan O yang menyebabkan tertundanya implementasi FMEA dalam rantai pasok.	Mengembangkan *tool* yang lebih komprehensif untuk semua tipe dari pengecekan dan perancangan platform FMEA untuk seluruh operasi rantai pasok.	panduan untuk industri manufaktur dalam memperbaiki masalah yang ada pada aplikasi FMEA, jadi perusahaan dapat mengadopsi proses FMEA dalam lingkungan kolaboratif.

(Estorilio & Posso, 2010)	Ada beberapa hasil FMEA yang tidak konsisten dalam teknik yang diterapkan pada pemasok otomotif.	FMEA *Process*	Masalah irregulariti es dan bertujuan untuk mengusulk an strategi untuk meminimal isir.	irregularities dalam proses FMEA dan mendapatkan 7 faktor yang dapat berkontribusi dalam ketidakkonsist ensian. Uji coba kepada 3 pemasuk, strategi tersebut dapat meningkatkan proses FMEA yang signifikan.	Meningkatka n strategi berdasarkan saran yang dikumpulkan dari pemasok. Dan dapat di lakukan uji coba pada sampel yang lebih besar dan memiliki banyak aktivitas operasional.	Teoritis : Mengkritisi metode FMEA, Praktis: strategi untuk perusahaan otomotif
(Xiao et al., 2011)	Penelitian ini mengenalkan metode baru yang secara langsung dapat menganalisa banyak kegagalan untuk sistem yang kompleks.	RPN	-	Metode yang diusulkan telah berhasil dikombinasika n dengan FMEA tradisional untuk mengukur reliabiliti sistem dalam model kegagalan yang banyak.	fokus dalam mengidentifi kasi dinamika FTA dengan memperhatik an kegagalan non eksponen.	Kontribusi dalam memodifikasi pengukuran risiko dengan RPN. Membantu para tim dalam melakukan pengukuran.
(Carlson, 2014)	Memberikan penjelasan singkat tentang konsep fundamental dan prosedur untuk FMEA yang efektif dan memberikan 6 sukses faktor FMEA	Sistem FMEA, Design FMEA, *Process* FMEA	-	Ketika FMEA digunakan dengan tepat, akan mengantisipasi dan mencegah masalah, mengurangi biaya, menurunkan waktu produksi, dan memperoleh keamanan dan tingginya reliabilitas produk dan proses.	Pengembang an sukses faktor lainnya yang mendukung kesuksesan aplikasi FMEA.	mendefinisika n 6 sukses faktor dan penjelasan lengkap mengenai FMEA yang dapat digunakan sebagai bahan baca untuk tim FMEA maupun yang baru mempelajari FMEA.
(Claxton & Campbel l-Allen, 2017)	Banyak organisasi kesehatan menghadapi keterbatasan dan peningkatan kompleksitas.	FMEA, Manajem en kualitas	Menguji FMEA pada studi kasus rumah sakit	FMEA menghasilkan manfaat, untuk manajemen risiko prospektif dan	Membuat *scope* yang jelas dengan mendefinisik an skala untuk	Teoritis: penggunaan FMEA pertama kali pada kasus laboratorium.

	Sehingga perlu manajemen risiko untuk aksi pencegahan sebelum terjadinya kejadian.			kesuluruhan peningkatan proses.	melakukan pemrioritasan.	Praktis: pelaporan dan percobaan nasional laboraturium.(medical sektor)
(Sharma & Sharma, 2010)	Memodelkan, menganalisa dan memprediksi prilaku dari sistem industri dalam pengukuran yang realistik dan konsisten dan merencanakan pemeliharaan yang cocok sesuai dengan strategi	*Root Cause Analysis*(RCA), FMEA, Fuzzy	Integrasi framework RCA, FMEA dan Fuzzy	Menggunakan FMEA tradisional dan sistem pendukung keputusan berbasis fuzzy menghilangkan ketidakpastian dan informasi subjektif.	-	Teoritis: Manajemen risiko dengan kualitatif (RCA dan FMEA) serta kuantitatif (fuzzy). Praktisi: Teknisi, Manager, Praktisi
(Sutrisno, Gunawan, Vanany, & Khorshidhi, 2016)	Modifikasi FMEA untuk menghitung risiko dari pemeliharaan limbah.	FMEA Modifikasi	Penambahan indikasi, pencegahan adn skala kontrol untuk mengatasi limitasi FMEA.	Kekurangan model yang diusulkan, dan perbaikan kembali dengan penambahan dimensi yang *extended.*	Model yang diusulkan masih terdapat kelemahan dari segi validitas dan kecocokan realita pada kasus.	Teoritis: Usulan model yang realistis Praktis: Metode Evaluasi risiko pemeliharaan limbah.
(Shahin, 2004)	Perhitungan Severity selama ini tidak dari pandangan pelanggan	FMEA, KANO, severity	Peningkatan kemampuan FMEA dengan KANO Model	Kesenjangan antara pelanggan dan manajer dalam memprioritaskan sekumpulan kekagagaln dan perbedaan antara RPN dan prioritisasi Cr disebabkan kesalahan frekuensi kejadian.	Menguji model pada sektor lainnya	Teoritis: Peningkatan FMEA Praktis: Manajer, desainer
(Paciarotti, Mazzuto, & D'Ettorre, 2014)	Modifikasi FMEA dan adaptasi *fit the quality control* fitur dan kebutuhan	FMEA, *Quality Control*	Revisi FMEA dengan konsep kegagalan menjadi konsep *defect.*	Prosedur komplit dan evaluasi pada nilai RPN yang paling penting.	Pengujian model pada sektor lain dengan memperhatikan faktor *friendly* yang di *claim.*	Teoritis: Modifikasi FMEA Praktis: Manager
(Lipol & Haq, 2011)	FMEA/FMECA metode analisis risiko yang	FMEA, FMECA	Penggunaan FMEA atau	FMEA lebih familiar dibandingkan	Dapat mengulas perbedaan	Teoritis: memberikan ulasan literatur

	digunakan industri.		FMECA serta perbedaannya dalam organisasi	FMECA dalam industri.	keduanya dan research berupa studi kasus.	dan studi kasus Praktis: Manajer
(Mason-Blakley & Habibi, 2014)	Masih kurangnya literatur tentang *Clinical Information Technology*(CIT) tentang risiko bahaya jika menerapkan teknologi ini.	FMEA, STPA, ISHA	Melakukan sintesis FMEA dari melihat kelemahan kualitatif.	Tiga kelemahan utama aspek kualitatif dari teknik yang mengkompromikan reproduktifitas : ruang lingkup analisis konsisten, pemodelan proses yang konsisten, dan kelengkapan model.	Penanganan faktor manusia dalam mode kegagalan dan tahap identifikasi efek perlu disistematisasi. Serta validasi model.	Teoritis: Mengusulkan ISHA (Information System Hazard Analysis) Praktis: Pedoman analis atau tim.
(Batbayar, Takács, & Kozlovszky, 2016)	Kombinasi *fuzzy* dan FMEA dalam mengevaluasi risiko dalam perangkat *software*pada bidang kesehatan.	Fuzzy, FMEA	FMEA tidak memadai untuk mengukur risiko yang berbeda.	Pendekatan *fuzzy* lebih akurat lebih akurat dengan melibatkan bobot dampak ahli yang berbeda	Memperhatikan pengukuran kualitatif dan kuantitiatif dalam pengukuran risiko.	Teoritis: kombinasi FMEA dan Fuzzy Praktis: Tim FMEA, Manajemen.
(Sawhney, Subburaman, Sonntag, Rao Venkateswara Rao, & Capizzi, 2010)	Modifikasi FMEA sehingga praktisi *lean* memahami dan meningkatkan reliabilitias dari sistem *lean.*	FMEA, Pegawai, Lean System	Modifikasi berdasarkan 4 kritikal sumber daya yaitu *personnel, equipment, materials*, dan *schedules*.	Metodologi praktikal untuk meningkatkan reliabiliti sistem *lean* adalah non eksisten. existent.	Database pengetahuan melibatkan banyak perhitungan yang membosankan dan karenanya perlu diotomatisasi.	Teoritis: Modifikasi FMEA dari 4 kritikal sumber daya Praktis: desainer sistem, manajerial.
(de Aguiar, Salomon, & Mello, 2015)	langkah terstruktur dari atribut proses FMEA, seperti potensi kegagalan, penyebab dan dampak, hal ini untuk membuat lebih mudah dalam mendefinisikan skor dan kontrol.	ISO 9001, *Process* FMEA	Perbandingan aplikasi konvensional FMEA dengan konsep yang diusulkan..	mempertimbangkan urutan kejadian dalam analisis kegagalan untuk memahami sebab dan akibatnya, sama seperti urutan input dan output	Mengukur dampak dari kejadian masing-masing kejanggalan dan menentukan klasifikasi dalam skala hirarki.	Teoritis: menunjukkan langkah yang lebih simpel, memfasilitasi tim dari berbagai disiplin. Praktikal: Dapat diterapkan pada

				dalam definisi pendekatan proses yang dibahas dalam ISO 9001.		pelaatihan.
(Liu, 2015)	Membangun FMEA yang baru untuk evaluasi, prioritisasi, dan peningkatan mode kegagalan.	FMEA, VIKOR, DEMATEL, AHP	Kombinasi VIKOR, DEMATEL dan AHP untuk menilai risiko mode kegagalan.	Model prioritas risiko baru dapat efektif dalam membantu analis menemukan mode kegagalan berisiko tinggi dan menciptakan strategi pemeliharaan yang sesuai.	Kombinasi FMEA dan Fuzzy. Metode yang objektif menentukan bobot faktor risiko yang tepat. Pengujian model pada studi kasus lainnya.	Teoritis: mengatasi kekurangan dan meningkatkan keefektifan FMEA tradisional. Praktis : panduan untuk analis.
(Lolli et al., 2016)	Modifikasi FMEA untuk membuat nilai untuk faktor kejadian lebih terpercaya, dan untuk menghubungkan grafik FMEA secara langsung ke aktivitas pemeliharaan	FMEA, Algoritma *clustering*, Quality Control	K-means bersamaan dengan pendekatan normalisasi, diterapkan dan dibandingkan untuk mengisi nilai kejadian.	FMEA yang direvisi ini memperbaiki standar karena formulasi matematika yang lebih ketat dan penerapannya yang saksama di lingkungan operasi yang sebenarnya.	Ditingkatkan dengan analisis statistik yang lebih dalam dan menerapkan teori fuzzy	Teoritis: pendekatan ini menunjukkan potensi yang tinggi untuk menghadapi masalah nyata. Praktis:Analis atau Tim FMEA.
(Jain, 2017)	Menggunakan FMEA pada proses manajemen dari instansi kesehatan.	FMEA, Healthcare	Menguji FMEA yang banyak terbukti menjadi metode yang efektif.	Terdapat limitasi FMEA seperti memakan waktu yang lama, tim yang multidisiplin, dsb. FMEA terbukti dapat meningkatkan proses manajemen yang sesuai dengan strategi dan prosedur.	Diperlukan untuk mengembangkan rencana mitigasi dan menerapkannya.	Teoritis: Membuktikan FMEA metode risiko yang relevan Praktis: Petunjuk penggunaan FMEA.
(Chang, 2009)	Pendekatan baru untuk meningkatkan kemampuan penilaian FMEA.	FMEA, Data Analisis, Manajemen Kinerja	Data Envelopment Analysis (DEA) dan menyelidiki SOD	Melalui contoh ilustrasi pendekatan yang diusulkan	Perlu dibahas jika satu atau lebih SOD tidak dapat dirubah; atau	Teoritis: Pendekatan baru DEA dan SOD pada FMEA. Praktis :

			sebagai pengganti RPN.	mendukung proposisi bahwa DEA tidak hanya dapat melengkapi FMEA tradisional untuk meningkatkan kemampuan penilaian.	beberapa interaksi terjadi dalam SOD. Selain pengaturan perangkat lunak dapat diinvestigasi lebih lanjut.	manajer, desainer.
(Zheng, Chin, & Wei, 2013)	Kebanyakan proses FMEA menggunakan form yang tidak efektif mengekspresikan, mengorganisasi, dan mengutilisasi pengetahuan kegagalan dari proses produksi selama perencanaan proses.	FMEA, *Knowledge-based approach*	Merepresentasikan model *knowledge-enriched* untuk meningkatkan proses FMEA dalam perencanaan proses.	Efektif menggambarkan pengetahuan FMEA proses dibandingkan spesifik proses kegagalan atau data.	Memvalidasi model pada studi kasus lainnya.	Teoritis: Model peningkatan FMEA proses Praktis: perencana, analis
(Thurnes, Zeihsel, Visnepolschi, & Hallfell, 2015)	Kombinasi Anticipatory Failure Determination(AFD) -FMEA atau disebut *Failure Mode and Effects Anticipation and Analysis* (FMEAA).	FMEA, AFD	kombinasi keuntungan dari kedua metode, menawarkan sinergi, dan memperluas potensi adopsi industri dengan menyediakan satu alat yang diuraikan.	cara baru untuk mengidentifikasi struktur dan kegagalan sistem mirip dengan cara yang biasa.	Mengadaptasi TRIZ untuk optimasi	Teoritis: Mengusulkan FMEAA Praktis: analis
(Cameron et al., 2017)	Proses identifikasi *hazard* dan kemungkinan definisi skenario pada kegagalan.	HAZOP, FMEA	Melakukan review tentang HAZOP dan FMEA	Menghasilkan 3 RQ, yaitu tentang meningkatkan efektifitas,efisiensi dan kemungkinan risiko *hazard* menggunakan HAZOP dan FMEA.	Sistem yang bekerja, *round robin* dan perbandingan dengan hasil dari praktis yang sekarang akan membantu kasus bisnis dengan HAZOP dan FMEA.	Teoritis: Isu operasional manajemen risiko Praktis: operasional, industri.

(Jacob, 2015)	Meningkatkan menemukan *root-cause* dari kegagalan komponen elektronik dari system-related failure anamnesis approach.	FMEA, reliabiliti, anamnesis	FMEA menganalisa pada level perangkat, maka diusulkan untuk level sistem.	Prosedur yang berguna, tetapi juga menampilkan hal-hal penting, seperti prose, kebutuhan tim interdisiplin, panduan, dan sebagainya. Proses 8D menjadi proses 10D akan mendukung implementasi dan inklusi dari tujuan kegagalan anamnesis.	Menguji pada studi kasus lainnya.	Teoritis: identifikasi risiko keseluruhan sistem. Praktis:analis kegagalan perangkat.
(Lai & Chin, 2014)	FMEA pada umumnya digunakan pada industri manufaktur. Dan adanya keterbatasan FMEA.	FMEA, Information Security, siklus PDCA	Mengembangkan FMEA pada bidang keamanan informasi dan perbaikan metodologi FMEA tradisional	Metodologi FMEA yang dimodifikasi terbukti efektif sebagai metodologi pengukuran risiko.	Klasifikasi aset informasi, dan evaluasi skala.	Teoritis: Menyediakan metodologi FMEA pada bidang keamanan informasi Praktis: Tim FMEA

Sumber: (Olahan peneliti, 2017)

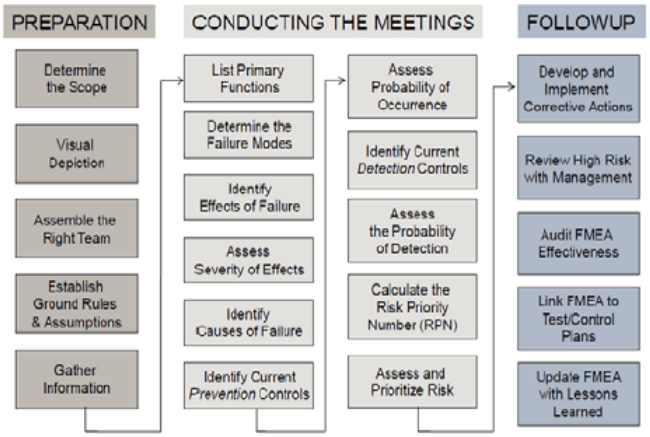
2.2.3 Acuan Utama Penelitian Terdahulu

Dalam mensintesis ataupun memformulasikan kerangka FMEA, diperlukan landasan atau acuan utama setiap kerangka pada FMEA. Berikut ini adalah acuan utama dari penelitian terdahulu yang digunakan:

Tabel 2.8 Acuan Utama Penelitian

1	Nama Peneliti	M.T. Odenholf, J.F. van Leeuwen, M.J. Nauta, D. de Kaste, Y.M.C.F. Odekerken-Rombouts, M.J. Vredenbregt, M. Weda, D.M. Barends.(Oldenhof et al., 2011)
	Judul Penelitian	*Consistency of FMEA used in the validation of analytical procedures*
	Tujuan	Untuk melakukan eksplorasi konsistensi dari hasil FMEA

		dalam validasi pada prosedur analitik, yang dilakukan oleh dua tim yang berbeda.
	Metodologi	1. Melakukan analisis risiko berdasarkan step yang telah didefinisikan sebelumnya pada dua tim yang berbeda. 2. Masing-masing tim memberikan skala skor untuk nilai *severity, occurrence,detection.* 3. Melakukan kalkulasi RPN pada masing-masing tim. 4. Melakukan perbandingan hasil dari RPN masing-masing tim.
	Hasil dan kesimpulan	Hasil dari penilaian risiko dari dua tim berbeda terbukti secara jelas tidak konsisten. Sehingga, kesimpulan yang didapatkan dari hasil adalah bahwa FMEA konsistensisnya dapat ditingkatkan dengan selalu dilakukan di bawah pengawasan fasilitator FMEA berpengalaman dan tim paling sedikit dua anggota dengan kompetensi dalam metode analisis yang akan divalidasi. Namun, FMEA dari Kedua tim berisi informasi berharga yang tidak diidentifikasi oleh tim lain, menunjukkan bahwa Ketidak konsistenan ini tidak selalu menjadi kelemahan.
	Hubungan dengan penelitan	Dari penelitian ini, membuktikan bahwa penerapan FMEA tradisional tidak konsisten. Sesuai dengan isu yang diangkat oleh peneliti terkait konsistensi FMEA, yang mana penilaiannya dilakukan oleh dua tim yang berbeda pada studi kasus yang sama. Sehingga, penelitian ini mendukung dalam memperkuat isu konsistensi FMEA dan memberikan panduan dalam melakukan analisis konsistensi hasil risiko sehingga membantu dalam sintesis kerangka FMEA.
2	Nama Peneliti	Carl S. Carlson (Carlson, 2014)
	Judul Penelitian	*Understanding and Applying the Fundamentals of FMEAs*
	Tujuan	Untuk menjelaskan tentang konsep fundamental dan prosedur untuk FMEA yang efektif dan memberikan 6 sukses faktor FMEA.

	Metodologi	
	Hasil dan kesimpulan	Ketika FMEA digunakan dengan tepat, akan mengantisipasi dan mencegah masalah, mengurangi biaya, menurunkan waktu produksi, dan memperoleh keamanan dan tingginya reliabilitas produk dan proses. Paper ini juga memberikan 6 sukses faktor: 1. Memahami fundamental dan prosedur FMEA termasuk konsep dan definisi. 2. Memilih proyek FMEA yang benar 3. Langkah persiapan untuk masing-masing proyek FMEA 4. Menerapkan pembelajaran dan sasaran 5. Menyediakan fasilitas yang 6. Mengimplementasikan sebuah proses FMEA yang efektif bagi perusahaan.
	Hubungan dengan penelitan	Membantu dalam mensintesis FMEA untuk memperoleh keamanan, reliabilitas, dan ekonomi produk ataupun proses. Sehingga, menjadi salah satu acuan yang digunakan untuk sintesis kerangka FMEA yang efektif.
3	Nama Peneliti	Carla Estorillio, Richard K. Posso(Estorilio & Posso, 2010)
	Judul Penelitian	*The reduction of irregularities in the use of "process FMEA"*
	Tujuan	Untuk mengidentifikasi iregularitas dan untuk mengusulkan strategi untuk meminimalkan konsistensi FMEA.

	metodologi	Memberikan kuisioner pada tujuh pemasok utama perusahaan otomotif eropa. Adapun tahapan dalam penelitian ini: 1. Memilih dasar teoritis 2. Memilih kasus 3. Mempersiapkan pemilihan data 4. Eksekusi : mengulas literatur, mengumpulkan data kuisioner dari pemasok, mengumpulkan data dari 10 proses FMEA. 5. Mempersiapkan laporan (diagnosis) 6. Saran untuk peningkatan : a. perubahan yang diusulkan (kerangka FMEA) dengan tahapan: analisis kritis dari masing-masing parameter, mendiagnosis kemungkinan penyebab dari parameter dan penyebabnya, dan membuat solusi peningkatan untuk metodologi dan kerangka kerja untuk meminimalisir kesalahan dalam menyiapkan FMEA. b. Validasi proposal perubahan kerangka
	Hasil dan kesimpulan	iregularitas dalam proses FMEA dan mendapatkan 7 faktor (pengetahuan, pelatihan, riwayat kegagalan, tim kerja dan sinergi, waktu yang dibutuhkan oleh metode, kontrol) yang dapat berkontribusi dalam ketidakkonsistensian. Uji coba kepada 3 pemasok, strategi tersebut dapat meningkatkan proses FMEA yang signifikan.
	Hubungan dengan penelitan	Penelitian ini mengkritisi konsistensi FMEA dengan melakukan perbaikan setiap tahapannya. Kemudian, dari penelitian ini diketahui 7 faktor yang dapat meminimalisir isu konsistensi.
4	Nama Peneliti	Lotto Kim Hung Lai, Kwai Sang Chin (Lai & Chin, 2014)
	Judul Penelitian	*Development of a Failure Mode and Effects Analysis Based Risk Assessment Tool for Information Security*
	Tujuan	Untuk membuat siklus FMEA keamanan informasi (*InfoSec FMEA Circle*) dengan memodifikasi metodologi FMEA tradisional.

	Metodologi	Mendemostrasikan kelayakan metodologi yang dikembangkan (*infoSec FMEA Circle*) sebagai kerangka yang dapat mengukur risiko keamanan informasi. Pengujian kerangka dilakukan pada studi kasus *Hong Kong Science and Technology Parks Corporation* (HKSTP).
	Hasil dan kesimpulan	Adapun tahapan yang diajukan terserbut adalah: 1. Tahap Perencanaan (Plan) 1.1. Memilih komponen keamanan informasi untuk dianalisis 1.2. Memilih poin kontrol untuk proses alir informasi 1.3. Mengidentifikasi potensial mode kegagalan pada poin/proses kontrol yang dipilih 1.4. Mengidentifikasi dampak pada mode potensi kegagalan 2. Tahap Pelaksanaan (Do : Identifikasi dan Analisis) 2.1. Identifikasi potensi dampak 2.2. Estimasi frekuensi atau kemungkinan dari terjadinya setiap mode potensi kegagalan 2.3. Evaluasi kemampuan mendeteksi potensi kegagalan 2.4. Menghitung RPN 3. Tahap Tindakan(Act: *Treat* dan *Review risk*) Setelah implementasi pada studi kasus, metodologi ini terbukti efektif dalam mengukur risiko keamanan informasi.
	<u>Hubungan dengan penelitan</u>	Penelitian ini memberikan masukan dalam perbaikan FMEA tradisional yang akan disintesis. Dengan melihat tahapan dalam pembuatan metodologi FMEA infosec circle menjadi gambaran bahwa FMEA merupakan kerangka yang masih perlu di eksplore terutama pada bidang teknologi informasi.

Pada tabel 2.8 menunjukkan acuan utama yang digunakan pada penelitian ini. Acuan utama ini merupakan hasil penyaringan dari jurnal yang telah diulas sebelumnya. Dari jurnal yang didapatkan, diketahui bahwa sebagian besar metode FMEA ini dimanfaatkan pada sektor industri manufaktur ataupun otomotif.

Sehingga, penelitian ini memiliki kontribusi dalam pembahasan FMEA pada bidang teknologi dan sistem informasi. Penelitian yang dipaparkan diatas memiliki kesenjangan yaitu belum adanya penelitian yang menganalisis konsistensi FMEA tradisional dan memberikan perbaikan serta strategi pada kerangka FMEA pada bidang teknologi informasi.

2.2.4 Konsistensi FMEA dan Dampaknya

Penggunaan yang tepat dari FMEA dapat memberikan beberapa manfaat seperti tingginya reliabilitas produk, pengurangan modifikasi rancangan, kualitas perencanaan yang lebih baik, peningkatan secara berkelanjutan pada produk dan perancangan proses, dan rendahnya biaya produksi, kemudian dapat memenuhi kebutuhan dari pelanggan (Gary Teng et al., 2006). Menurut (Lai & Chin, 2014), sebagian besar dari metode ataupun *tools* dari manajemen risiko adalah kualitatif dan deskriptif. FMEA diklasifikasikan dalam semi kuantitatif. Sehingga selama proses FMEA, angka RPN dari potensial kegagalan dapat mendukung analisis kuantitatif dari kejadian risiko, dan metode ini bukan hanya menemukan tingkat tinggi risiko secara tepat daan cepat, tetapi juga mengatasi kekhawatiran kehilangan dan meningkatkan reliabilitas sebuah produk ataupun jasa(Zhao & Bai, 2010). Tidak seperti prosedur pengukuran risiko lainnya, FMEA dapat mengevaluasi secara kritis dari risiko yang potensial (Murphy et al., 2011). FMEA menghasilkan manfaat, untuk manajemen risiko prospektif dan kesuluruhan peningkatan proses.Hal ini berguna bagi manajemen untuk terus melakukan strategi manajemen inovasi dengan mengidentifikasi batasan dari prioritas risiko. FMEA juga berguna untuk manajemen risiko prospektif dan kesuluruhan peningkatan proses(Claxton & Campbell-Allen, 2017).

FMEA memiliki limitasi atau kekurangan berdasarkan literatur yang telah diulas dan adanya kesenjangan yang ditemukan. Permasalahan umum yang ada pada FMEA berdasarkan pengalaman (Gary Teng et al., 2006), bahwa kurangnya informasi yang rinci pada fungsi produk atau bagian, mode potensial kegagalan, potensi dampak dari kegagalan, potensi penyebab kegagalan, dan perancangan kontrol yang ada. Sehingga, dengan kurangnya informasi ini menyebabkan kesalahpahaman, kebingungan atau ketidakpastian dalam pendefinisian risiko.

Permasalahan lainnya adalah integritas dokumen FMEA yang termasuk permasalahan tidak konsistennya peringkat pada *severity, occurrence,* dan *detection,* yang beberapa bagian dari laporan FMEA hilang, tidak adanya rekomendasi untuk risiko yang tinggi berdasarkan RPN, dan perubahan skala dari peringkat setelah melakukan koreksi.

FMEA tradisional menggunakan pendekatan dengan skala linier untuk menentukan *severity, occurrence* dan *detection* dengan nilai angka. Kriteria skala ini menjadi permasalahan jika pendefinisian yang tidak jelas dan batasan yang meragukan. Penelitian (Paciarotti et al., 2014) melakukan modifikasi atau perbaikan dari segi skala FMEA. Hal ini dilakukan untuk meminimalisir kekurangan dari FMEA. Penelitian tersebut mendefinisikan skala (1,3,9) dalam pemberian nilai S, O, D dengan tingkat (*high, medium, low*). Membatasi ukuran variabel parameter dapat menjadikan FMEA menjadi metode yang lebih cepat, menjadi lebih efektif serta menghasilkan hasil yang kuat.

Terdapat isu subjektif dalam melakukan prioritisasi risiko, hal ini merupakan salah satu limitasi yang didapatkan berdasarkan literatur review yang telah dilakukan. Kegiatan prioritisasi dilakukan berdasarkan emosi manusia dan pikiran, sehingga terdapat keraguan dalam keakuratan konsep yang tentunya juga berasal dari parameter yang digunakan. Tim FMEA akan sulit menentukan perbedaan opini yang terjadi dalam perhitungan, dan variabel yang dibutuhkan dalam menghitung angka risiko yang tidak sesuai dan meragukan (Kakvan et al., 2014). Subjektivitas individual dan bias juga berdampak pada dinamika tim. Kesalahan pendefinisian risiko bergantung pada pengalaman anggota tim dalam menganalisis kegagalan dan familiarnya sistem bagi anggota serta bias kognitif yang diketahui. Dengan demikian, sangat adanya kemungkinan kesalahan manusia. Situasi ini sering terjadi bila sedikit data mengenai kejadian dan efek kegagalan diketahui, sehingga memerlukan subjektivitas(Banghart, 2014). Dari hasil yang tidak konsisten disebabkan oleh subjektifitas ini sehingga perlu adanya strategi untuk mengatasi subjektifitas tim FMEA dalam melakukan penilaian risiko.

FMEA yang memakan waktu dalam proses membutuhkan tim yang multidisiplin sehingga memahami dengan baik proses yang dianalisa. FMEA

hanya membantu dalam mengidentifikasi kemungkinan proses yang gagal, tetapi tidak mengeliminasinya, sebagai tambahan perlu adanya usaha untuk membangun rencana aksi dan mengimplementasikannya(Jain, 2017). Jadi, tidak hanya mampu menggunakan FMEA tetapi juga mengimplementasikan aksi perbaikan.

Konsistensi hasil FMEA dapat ditingkatkan dengan membangun keahlian dari beberapa fasilitator yang dapat membantu tim analis untuk menggunakan FMEA supaya lebih efektif dan konsisten dengan mendefinisikan mode kegagalan dan tingkat keparahan, kemungkinan dan indeks yang terdeteksi. Kemudian, dengan pengalaman fasilitator akan membuktikan nilai ketika mengevaluasi dampak dari aksi perbaikan yang telah dilakukan. Strategi kedua yang mungkin dilakukan adalah selalu adanya anggota teknisi ahli dalam sebuah tim, hal ini berdampak pada pemberian nilai. Paling sedikit ada dua teknisi ahli yang termasuk dalam tim FMEA untuk menyeimbangkan perbedaan individu yang signifikan dalam keputusan risiko yang krusial (Oldenhof et al., 2011). Strategi lainnya adalah dengan mengkombinasikan FMEA dengan metode lainnya. Dari literatur yang di dapat metode *Fuzzy* adalah yang paling banyak digunakan dalam modifikasi FMEA. Menggunakan FMEA tradisional dan sistem pendukung keputusan berbasis *fuzzy* menghilangkan ketidakpastian dan informasi subjektif(Sharma & Sharma, 2010).

Berdasarkan *literature review* yang telah dilakukan oleh (Liu, Liu, & Liu, 2013) bahwa penggunaan *fuzzy* pada kerangka FMEA memiliki kekurangan. Pertama, sulitnya mendefinisikan fungsi-fungsi yang relevan untuk faktor risiko karena bahasa atau istilah yang sulit dipahami dengan mudah. Kedua, membutuhkan biaya yang besar dan memakan banyak waktu dalam penerapan *fuzzy*. Ketiga, perhitungan yang kompleks dengan mempertimbangkan kehilangan informasi yang banyak dalam proses analisis risiko. Sehingga, penerapan *fuzzy* pada kenyataannya masih sulit dan membutuhkan waktu yang lama dalam proses analisis risiko.

Menurut Backlund dan Hannu (2002), telah banyak sejumlah subjektif pendekatan manajemen risiko, tetapi semuanya memiliki limitasi seperti tidak bisa menghasilkan dukungan keputusan yang konsisten dan relevan. Bukan berarti pendekatan yang murni menggunakan kuantitatif terbebas dari permasalahan.

Manajemen risiko yang subjektif tentunya secara jelas adalah limitasi yang perlu diperhatikan. Termasuk yang ada pada FMEA yang merupakan salah satu pendekatan dalam manajemen risiko.

Setiap organisasi menginginkan pendukung dalam produk dan proses dari segi keamanan, bebas masalah selama menjalankan kegiatan bisnis. Ketika FMEA digunakan secara tepat, maka FMEA dapat mengantisipasi dan mencegah masalah, mengurangi biaya, mempersingkat waktu produksi, dan mencapai keamanan dan produk/jasa yang terpercaya (Carlson, 2014). Akan tetapi, jika FMEA digunakan secara tidak tepat ataupun terdapatnya hasil yang tidak konsisten, tentunya akan memberikan kerugian pada organisasi. Hal ini dikarenakan, seharusnya prioritas risiko membutuhkan biaya yang lebih besar pada risiko peringkat tertinggi, akan tetapi dengan adanya perbedaan peringkat risiko maka organisasi bisa saja melakukan kesalahan dalam pencegahan atau fokus penanganan.

Akan tetapi, tidak selalu hasil risiko yang tidak konsisten pada FMEA mengindikasikan kelemahan yang buruk pada prosedur analisis risiko. FMEA yang dilakukan oleh dua tim yang berbeda akan memberikan informasi yang bernilai yang tidak diidentifikasikan oleh tim lainnnya (Oldenhof et al., 2011). Perbedaan tersebut menimbulkan pendefinisian risiko baru yang sebelumnya tidak ada. Sehingga, masing-masing tim FMEA akan diberikan kebebasan dalam menggunakan pendekatan FMEA ini secara fleksibel untuk mendefinisikan risiko yang ditemukan.

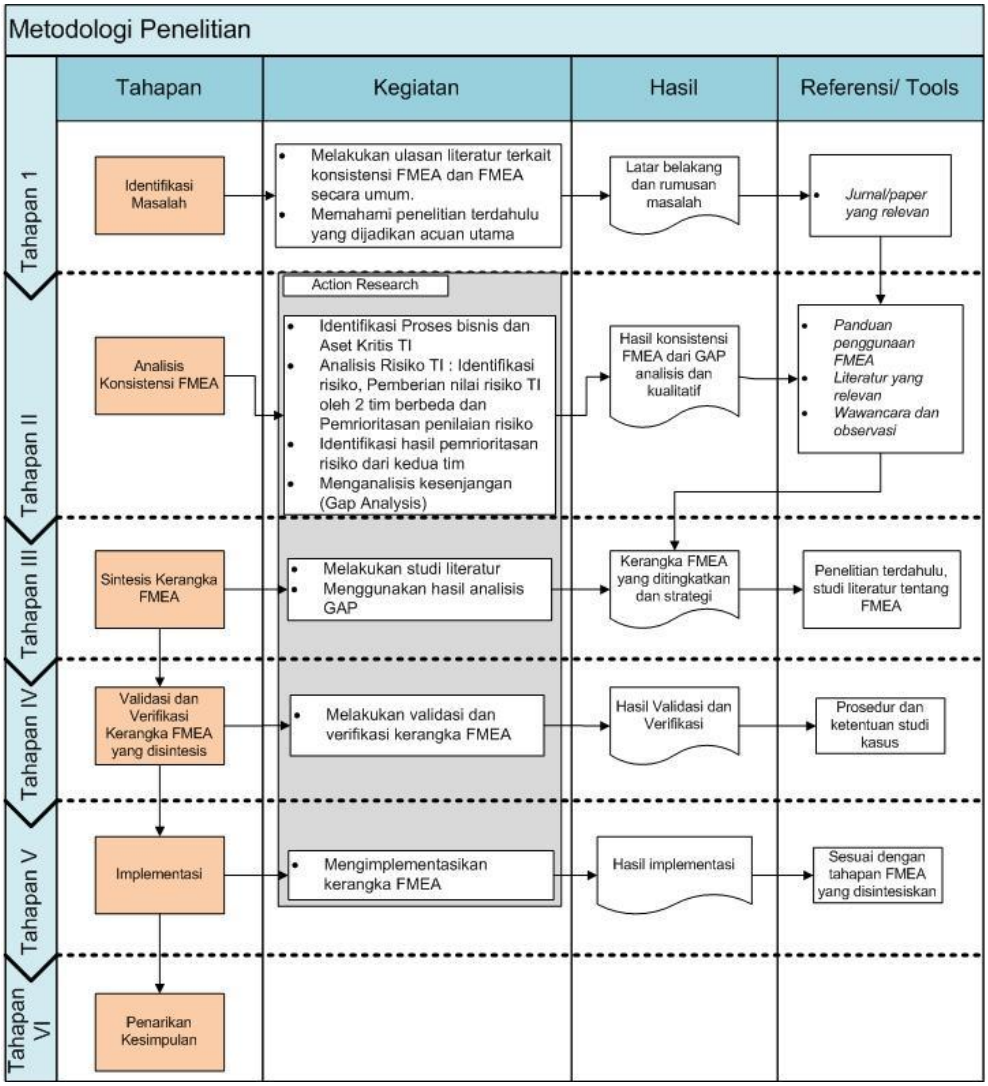
(*Halaman ini sengaja dikosongkan*)

BAB 3
METODOLOGI PENELITIAN

Bab ini akan menjelaskan langkah-langkah yang diperlukan dalam prosespenelitian sebagai kerangka acuan dalam proses pengerjaan tesis, sehinggarangkaian pengerjaan dapat dilakukan secara terarah, teratur, dan sistematis.

3.1. Tahapan Penelitian

Tabel 3.1. Tahapan penelitian



Sumber: (Olahan Peneliti, 2018)

3.2 Identifikasi Masalah

Tujuan dari pengidentifikasian masalah yaitu untuk menemukan *research question* penelitian yang telah dibahas pada bagian sebelumnya. Identifikasi masalah didasarkan pada studi penelitian terdahulu dan ditemukannya kesenjangan (*gap*) yang dapat menjadi celah penelitian selanjutnya. Permasalahan yang diangkat pada penelitian ini merupakan isu konsistensi FMEA dalam manajemen risiko. Adapun kesenjangan yang didapatkan adalah belum adanya pembuktian konsistensi secara jelas pada tahapan FMEA tradisional dan sekaligus strategi untuk meminimalisir isu konsistensi. Sehingga, penelitian ini nantinya akan menghasilkan FMEA yang ditingkatkan (FMEA *Improvement*) dan menguji coba kerangka tersebut ke studi empiris.

3.2.1. Studi Kasus Penelitian

Lokasi penelitian dilakukan pada Kantor Wilayah Kementerian Agama (Kanwil Kemenag) Provinsi Riau. Kanwil Kemenag salah satu tugas pokoknya adalah melakukan pembinaan dan pelayanan di bidang agama dan keagamaan di Provinsi Riau, sekaligus berfungsi melakukan dan menjabarkan kebijakan Menteri Agama Republik Indonesia di Provinsi Riau. Kanwil Kemenag Provinsi Riau, merupakan instansi vertikal Kementrian Agama (tidak termasuk yang diotonomikan), berada di bawah dan bertanggungjawab langsung kepada Menteri Agama.

Kanwil Kemenag Riau telah menggunnakan Teknologi Informasi dalam proses bisnisnya. Pengadopsian berbagai layanan berbasis TI dilakukan oleh Kanwil Kemenag Riau sebagai strategi dalam pencapaian tujuan organisasi dan tentunya peningkatan pelayanan pada masyarakat.Sehingga, pada penelitian ini dilakukan implementasi kerangka FMEA tradisional maupun kerangka FMEA yang telah disintesis sebagai pembuktian konsistensi dan menjadi validasi empiris pada Kantor Kemenag Riau. Pengujian kerangka FMEA akan mengikuti alur dari metodologi yang telah dideskripsikan pada penelitian ini.

3.3 *Action research*

Penelitian ini menggunakan metode *action research* yang terbagi menjadi dua siklus dilakukan dengan proses sebagai berikut (Rose et al., 2015):

1. Siklus 1 (*Plan, Act, Observe, Reflect*): Implementasi Kerangka FMEA Tradisional. Pada siklus ini dilakukan kontrol dalam pengimplementasian kerangka FMEA tradisional yang diujikan pada dua tim yang berbeda pada satu studi kasus. Tahapan ini bertujuan untuk menganalisis konsistensi dari FMEA tradisional. penjabaran dari setiap siklus tahapan adalah sebagai berikut:
    a. *Plan.* Perencanaan dilakukan untuk mendesain skenario penilaian risiko yang dilakukan dengan FMEA tradisional. Tahapan ini sebagai input untuk tahapan selanjutnya.
    b. *Act.* Dalam penelitian aksi ini, peneliti turut ikut terjun dan terlibat secara langsung di dalam menerapkan skenario penelitian bersama partisipan yang terkait. Kegiatan ataupun proses yang dilakukan yaitu mengidentifikasi proses bisnis dan aset kritis Teknologi Informasi pada studi kasus. Kemudian, menganalisis risiko TI yang terdiri dari identifikasi risiko TI, pemberian nilai risiko oleh dua tim, pemrioritasan penilaian risiko, dan perbandingan hasil risiko.
    c. *Observe.* Peneliti mengumpulkan data-data dari hasil penerapan skenario penelitian selama pelaksanaan *action research* berlangsung. Pengumpulan data yang dibutuhkan tersebut akan menjadi input peneliti dalam menganalisa hasil untuk proses selanjutnya.
    d. *Reflect.* Pada tahapan ini dilakukan analisis kesenjangan (*Gap Analysis*). Analisis kesenjangan dilakukan sebagai inti analisis konsistensi hasil risiko TI dengan melihat perbedaan hasil RPN yang didapatkan oleh kedua tim. Hasil analisis ini menjadi input pada siklus selanjutnya untuk perbaikan FMEA.

Tahapan pada masing-masing siklus dijelaskan secara lebih detail dijelaskan pada subbab selanjutnya.

2. Siklus 2 (*Plan, Act, Observe, Reflect*): Implementasi Kerangka FMEA yang disintesis. Pada siklus kedua ini dilakukan kontrol dalam pengimplementasian

kerangka FMEA yang telah disintesis dan kemudian diujikan pada dua tim yang berbeda pada satu studi kasus.Adapun penjabaran dari setiap siklus tahapan adalah sebagai berikut:

a. *Plan.* Perencanaan dilakukan untuk mendesain penilaian risiko yang dilakukan dengan FMEA Kerangka FMEA yang disintesis. Secara umum, kegiatan ini dilakukan untuk mendesain skenario penelitian. Skenario penelitian tersebut nantinya diterapkan secara langsung ke objek penelitian bersama dengan partisipan terkait untuk kemudian dilakukan pengamatan. Perumusan skenario yang dilakukan tersebut akan memperhatikan aspek kemungkinan untuk dapat diterapkan dan diamati hasilnya selama kurun waktu penelitian. Detail kegiatan pada tahapan sintesis kerangka FMEA dijabarkan pada subbab sintesis kerangka FMEA.
b. *Act.* Dalam penelitian aksi ini, peneliti turut ikut terjun dan terlibat secara langsung di dalam menerapkan skenario penelitian bersama partisipan yang terkait. Kegiatan ataupun proses yang dilakukan dengan mengimplementasikan kerangka FMEA yang telah disintesis pada studi kasus.
c. *Observe*. Peneliti mengumpulkan data-data dari hasil penerapan skenario penelitian selama pelaksanaan *action research* berlangsung. Pengumpulan data yang dibutuhkan tersebut akan menjadi input peneliti dalam menganalisa hasil untuk proses selanjutnya.
d. *Reflect.* Pada tahapan ini menganalisis perbedaan hasil yang didapatkan dari kedua tim untuk melihat kesenjangan RPN. Hal ini dilakukan sebagai analisis hasil penelitian dan penarikan kesimpulan.

Tahapan pada masing-masing siklus dijelaskan secara lebih detail dijelaskan pada subbab selanjutnya.

Dari penerapan kedua siklus tersebut, akan dilihat perbedaan kerangka FMEA tradisional dengan FMEA yang telah dilakukan perbaikan. Perbedaan tersebut dilihat berdasarkan perbedaan peringkat yang didapatkan oleh kedua tim pada kedua siklus tersebut. Sehingga, hasil yang diharapkan adalah kerangka

FMEA yang telah diperbaiki akan menghasilkan kesenjangan yang semakin kecil pada pemrioritasan risiko kedua tim.

3.4 Analisis Konsistensi FMEA

Dalam melakukan analisis konsistensi FMEA akan melalui beberapa tahapan. Berikut ini adalah penjelasan masing-masing tahapan.

3.4.1 Identifikasi Proses Bisnis dan Aset Kritis

Sebelum pendefinisian aset kritis, dilakukan analisis proses bisnis yang ada pada studi kasus. Identifikasi aset kritis dilakukan untuk mengetahui aset teknologi informasi yang dimiliki oleh studi kasus yang akan diteliti. Sehingga, dengan mengidentifikasi aset kritis dapat didefinisikan dan membentuk daftar risiko yang akan dianalisis. Identifikasi aset kritis dengan cara mengumpulkan data-data terkait dengan kondisi eksisting dari studi kasus. Tahapan dalam mengidentifikasi kondisi eksisting tersebut adalah dengan membangun profil ancaman berbasis aset (identifikasi aset kritis, identifikasi kebutuhan keamanan aset, identifikasi ancaman, identifikasi keamanan yang sudah diterapkan, identifikasi kelemahan organisasi), kemudian dilakukan identifikasi kerentanan infrastruktur (identifikasi komponen utama, identifikasi kelemahan teknologi yang sudah ada) (Alberts & Dorofee, 2002). Langkah dalam mengumpulkan data untuk identifikasi proses bisnis dan aset kritis adalah sebagai berikut:

1. Observasi Lapangan

Merupakan suatu metode yang sangat efektif karena langsung mengadakan pengamatan pada kegiatan yang sesuai dengan materi penelitian. Mencari dan menentukan lokasi penelitian secara mandiri turun langsung kelapangan, tempat penelitian adalah riil, bukan fiktif atau dibuat- buat, kemudian menganalisa tempat yang akan dituju. Observasi dilakukan dengan cara melakukan pengamatan proses bisnis yang ada pada studi kasus.

2. Wawancara

Wawancara yaitu kegiatan tanya jawab secara lisan antara peneliti dengan informan secara langsung. Wawancara dilakukan untuk memperoleh data untuk kelengkapan data-data yang diperoleh sebelumnya.

3. Dokumentasi

Dokumentasi dalam pengumpulan data dimaksudkan untuk mendokumentasikan seluruh data yang didapatkan baik melalui wawancara maupun observasi. Dokumentasi hasil wawancara dilakukan dengan merekam percakapan dengan informan dan mencatat hasil wawancara dengan informan.

3.4.2 Analisis Risiko TI

Dalam menganalisis konsistensi FMEA ini dilakukan dengan metodologi yang dikembangkan oleh (Oldenhof et al., 2011), seperti tahapan dibawah ini.

Gambar 3.1 Tahapan Analisis Konsistensi FMEA

Sumber : (Oldenhof et al., 2011)

Penelitian yang dilakukan oleh Oldenhof et al (2011) menguji konsistensi FMEA dengan pemberian nilai risiko dari dua tim yang berbeda pada satu studi kasus. Analisis risiko dilakukan dengan melakukan identifikasi penyebab, keparahan, dan kegagalan dari setiap peluang pada aset kritis yang telah didefinisikan sebelumnya. Berdasarkan prosedur FMEA, bahwa sebelum melakukan analisis risiko maka tim FMEA memberikan tata cara penilaian risiko sesuai prosedur.

3.4.2.1 Identifikasi Risiko

Identifikasi risiko atau *brainstorming failure* menggunakan metode FMEA bertujuan untuk mengetahui kegagalan yang dapat terjadi pada fungsi dalam sistem yang diterapkan. Tahapan awal dalam identifikasi risiko dilakukan dengan mengidentifikasi ancaman (*threats*), kelemahan (*vulnerability*), dan kemungkinan insiden yang tidak diketahui (*attacks*)(Lai & Chin, 2014). Hasil akhir dari tahapan ini berupa daftar risiko disertai dampak, penyebab yang potensial pada aset studi

kasus dari kategori risiko *hardware, software, people,data,* dan *network* (Desy et al., 2014).

3.4.2.2 Pemberian/Pengukuran Nilai Risiko TI

Pengukuran nilai risiko bertujuan untuk memberikan nilai pada setiap risiko berdasarkan nilai *severity*, *occurence*, dan *detection* yang dilakukan oleh dua tim yang berbeda dalam satu studi kasus yang sama.

3.4.2.3 Pemrioritasan Penilaian Risiko TI

Risiko yang telah dinilai menggunakan parameter *severity, occurence*, dan *detection* akan dilakukan pemrioritasan risiko yang memiliki urgensi tertinggi. Pemrioritasan penilaian risiko menggunakan RPN, sehingga didapatkan hasil risiko yang telah dikategorikan berdasarkan level risiko (*very high, high, medium, low,* dan *very low*). Penelitian analisis konsistensi risiko dengan cara membuat dua tim yang berbeda untuk mengidentifikasi risiko yang sama pada satu perusahaan. Kemudian membandingkan hasil peniliaian yang didapatkan apakah sudah konsisten atau belum.

3.4.2.4.Perbandingan hasil risiko dari Kedua Tim

Hasil penilaian risiko yang dilakukan dari dua sudut pandang yang berbeda pada studi kasus perusahaan yang sama. Hasil yang didapatkan dari tahapan ini adalah perbedaan penilaian risiko dari masing-masing tim.

3.4.3. Analisis Kesenjangan (Gap Analysis)

Analisis kesenjangan dilakukan untuk melihat perbedaan yang terjadi antara penilaian yang dilakukan oleh dua tim yang berbeda, dan memberikan usulan perbaikan. Usulan perbaikan akan menjadi landasan bagi tahapan sintesis kerangka FMEA yang ditingkatkan. Sehingga, analisis ini dapat mengahasilkan kesimpulan yang didapatkan untuk mengidentifikasi konsistensi penggunaan metode FMEA dalam melakukan penilaian risiko.

3.5 Sintesis Kerangka FMEA (*FMEA Improvement*)

Sintesis Kerangka FMEA yang ditingkatkan ini menggunakan hasil analisis *gap* dari hasil penilaian risiko dari dua tim berbeda. Kemudian, pada tahapan ini juga dilakukan studi literatur terkait FMEA. Studi literatur dalam penelitian ini bersumber dari buku, media, ataupun dari hasil penelitian orang lain. Pemahaman terhadap literatur bertujuan untuk menyusun dasar teori terkait yang digunakan dalam melakukan penelitian. Studi literatur selain digunakan untuk membantu peneliti mulai dari merumuskan permasalahan hingga penyusunan tesis, juga digunakan untuk menentukan sintesis kerangka FMEA yang ditingkatkan.Pada tahapan ini juga melakukan studi banding *best practice* dan standar yang ada terkait manajemen risiko TI. Hasil dari kerangka FMEA ini sebagai rekomendasi dalam limitasi dari FMEA. Adapun tahapan sintesis yang dilakukan secara lebih detail sebagai berikut(Estorilio & Posso, 2010):

1. Kritikal analisis pada setiap proses/parameter yang diidentifikasi. Pada tahapan ini mengidentifikasi variabel yang menjadikan tidak konsistennya hasil FMEA yang diperoleh. Hasil tahapan ini berupa kelemahan FMEA yang perlu diperhatikan pada proses FMEA.
2. Mendiagnosis kemungkinan penyebab yang mempengaruhi parameter. Pada tahapan ini melakukan studi literatur terkait kemungkinan penyebab terjadinya kelemahan tersebut. Hasil analisis gap akan menjadi acuan tambahan untuk memperkuat diagnosa penyebab kelemahan tersebut.
3. Memberikan usulan perbaikan pada tahapan FMEA. Pada tahapan ini memberikan rekomendasi solusi untuk meminimalisir kelemahan yang dideteksi berdasarkan fakta yang ditemukan pada studi kasus (analisis gap). Kemudian, studi literatur terkait perbaikan proses FMEA termasuk strategi tiap prosesnya agar FMEA dapat ditingkatkan dalam pengimplementasiannya pada studi kasus.

3.6 Validasi

Validasi dilakukan dengan menerapkan kerangka FMEA tradisional dan yang telah disintesis pada studi kasus yang disesuaikan dengan prosedur dan kebijakan studi kasus tersebut. Verifikasi dilakukan dengan mendapatkan

konfirmasi dari pihak manajemen bahwa konsep kerangka yang disintesis telah sesuai dengan kebijakan dan prosedur dari studi kasus. Validasi dilakukan secara bertingkat. Pada tahapan awal, validasi dokumen FMEA tradisional dilakukan oleh dua orang praktisi TI, kemudian validasi dokumen FMEA yang telah disintesis dilakukan oleh pakar dalam bidang manajemen risiko.

3.7 Implementasi Kerangka FMEA *Improvement*

Implementasi ini sebagai validasi empiris dari kerangka FMEA yang telah disintesis. Pengujian kerangka FMEA dilakukan dengan mengikuti alur metodologi yang telah dibuat. Hasil dari simulasi dari proses analisis risiko ini akan menunjukkan kebenaran (valid) dan kecukupan kerangka yang telah disintesis. Hasil yang diperoleh nantinya juga membandingkan kesenjangan yang diperoleh setelah kerangka FMEA yang ditingkatkan dengan sebelumnya. Penilaian kerangka FMEA yang disintesis dilakukan dengan melibatkan praktisi manajemen risiko keamanan teknologi informasi. Adapun karakteristik dari praktisi yang dimaksudkan adalah:

1. Orang yang mengerti tentang keamanan teknologi informasi terutama risiko yang ditimbulkan pada keamanan teknologi informasi.
2. Orang yang pernah dan berpengalaman dalam menggunakan kerangka FMEA dalam menganalisa risiko TI.
3. Orang yang memiliki latar belakang pendidikan dalam ranah Teknologi atau Sistem Informasi.

3.8 Penarikan Kesimpulan

Tahapan terakhir dalam penelitian ini yakni menganalisis dan membahas temuan keseluruhan dalam penelitian, terkait dengan hasil analisa data yang diperoleh. Tahap penyusunan kesimpulan dilakukan dengan menelaah secara keseluruhan terhadap apa yang telah dilakukan pada penelitian ini. Kesimpulan dibuat berdasarkan hasil studi literatur, desain metode penelitian, validasi data, hasil analisis serta saran untuk peluang penelitian yang akan datang.

(*Halaman ini sengaja dikosongkan*)

BAB 4
HASIL DAN PEMBAHASAN

4.1. Siklus 1. *Action research* FMEA Tradisional

Berikut ini penjabaran hasil dari siklus pertama dalam *action research* FMEA tradisional. Implementasi FMEA tradisional dilakukan dengan mengikuti metodologi yang telah didefinisikan pada BAB sebelumnya.

4.1.1. Skenario *Action research* 1

Skenario yang dideskripsikan pada tabel 4.1. adalah panduan dalam melakukan *action research* untuk siklus pertama. Skenario dilakukan sebagai kontrol peneliti dalam melakukan penelitian. Tahapan proses dimulai saat melakukan analisis konsistensi FMEA dengan mengimplementasikan FMEA tradisional pada studi kasus. Pengimplementasian FMEA tradisional dilakukan pada Kantor Wilayah Kementerian Agama Provinsi Riau. Fokus penelitian dilakukan pada Bidang Penyelenggaraan Haji dan Umrah. Pada bidang tersebut menggunakan Sistem Komputerisasi Haji Terpadu Generasi 2 (SISKOHAT Gen 2) yang merupakan aset kritis.

FMEA tradisional digunakan oleh dua tim yang berbeda. Tim pertama terdiri dari kepala seksi SISKOHAT dan dua orang fasilitator. Tim kedua terdiri dari pegawai senior/pegawai operasional dan dua orang fasilitator. Fasilitator yang adalah orang yang menyediakan perangkat pengukuran dan mengukur risiko IT. Fasilitator terdiri dari peneliti dan dua orang praktisi risiko TI. Sebelum dilakukan pengukuran risiko oleh kedua tim, terlebih dahulu dilakukan pengidentifikasian proses bisnis yang berjalan pada studi kasus. Selanjutnya dilakukan pengidentifikasian aset-aset kritis dan membangun profil berbasis ancaman.

Pada siklus pertama menghasilkan hasil analisis kesenjangan dari hasil pengukuran risiko oleh kedua tim. Kesenjangan dilihat berdasarkan perbedaan peringkat (ranking) dari RPN. Indikator perbedaan dianalisis dan memberikan usulan strategi akan menjadi input dalam siklus kedua dari *action research.* Siklus kedua menjadi solusi perbaikan dalam mengatasi isu konsistensi yang ditemukan pada siklus pertama.

Tabel 4.1. Skenario Siklus *Action Research* 1

Tahapan	Indeks Proses	Proses	Indeks Skenario	Skenario	Luaran yang Diharapkan	Data Skenario
Analisis Konsistensi FMEA / Implementasi FMEA Tradisional	P1	Identifikasi Proses Bisnis dan Aset Kritis. (aktor: peneliti dan Kepala divisi/ Pegawai senior)	P1.S1	Menganalisa proses bisnis yang ada pada studi kasus.	Aliran alur proses bisnis	- Profil Instansi - *Job desk* - Data wawancara
			P1.S2	Mengidentifikasi aset kritis.	Profil aset berbasis ancaman	- Data Aset TI - Dokumentasi Lapangan - Data wawancara
			P1.S3	Mengidentifikasi kebutuhan keamanan aset.		
			P1.S4	Mengidentifikasi ancaman yang mungkin terjadi dengan penerapan teknologi informasi.		
			P1.S5	Mengidentifikasi keamanan yang sudah diterapkan.		
				Mengidentifikasi kelemahan (*vulnerability*).		
			P1.S6	Mengidentifikasi komponen utama.	Daftar kerentanan infrastruktur	
			P1.S7	Mengidentifikasi kelemahan teknologi yang sudah ada.		
	P2	Analisis Risiko TI (aktor: Identifikasi Risiko: Peneliti; Pengukuran risiko : Peneliti, praktisi	P2.S1	Identifikasi risiko. Peneliti menyusun tabel yang diperlukan untuk pengukuran.	Daftar risiko yang siap untuk di ukur untuk kedua tim.	- Dokumen FMEA yang akan di uji - Lembar validasi dan verifikasi dokumen FMEA

		risk IT, Kepala Divisi, Pegawai operasional)	P2.S2	Meminta bantuan kepada pihak instansi untuk membentuk dua tim untuk mengukur risiko.	Terbentuknya tim 1 dan tim 2 untuk melakukan penilaian risiko	- Lembar pengesahan penunjukan tim FMEA
			P2.S3	Memberikan pengarahan atau petunjuk pengisian.	Kontrol dan interaksi peneliti dengan tim	- Dokumentasi - Petunjuk pengisian
			P2.S4	Penilaian risiko oleh dua tim.	Hasil pemberian nilai risiko oleh kedua tim	- Dokumen FMEA yang telah diisi atau diberi nilai - Dokumentasi surat bukti telah selesai penilaian.
			P2.S5	Perangkingan risiko dari kedua tim	Hasil RPN	- Dokumen RPN
	P3	Analisis Kesenjangan	P3.S6	Identifikasi dan analisis perbedaan hasil kedua tim	Indikator perbedaan dan hasil analisis gap berupa usulan perbaikan.	- Dokumen Hasil FMEA - Literatur - Data wawancara

Sumber: Olahan Peneliti, 2018

4.1.2. Identifikasi Proses Bisnis dan Aset Kritis

4.1.2.1.Analisis Proses Bisnis

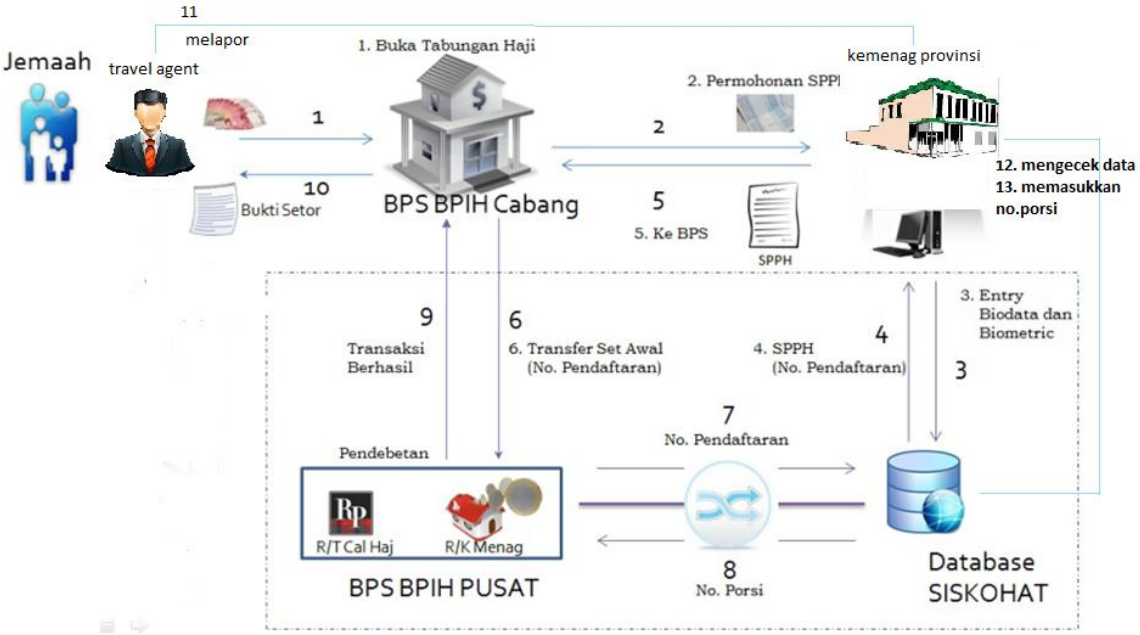
Bidang Penyelenggaraan Haji dan Umrah telah menggunakan Teknlogi Informasi dalam proses bisnisnya. Sistem yang digunakan oleh bidang ini adalah Sistem Komputerisasi Haji Terpadu (SISKOHAT). SISKOHAT pada tingkat provinsi merupakan sistem yang berguna untuk memonitor jemaah haji mulai dari pendaftaran, pemberangkatan hingga pemulangan jemaah haji.SISKOHAT yang diterapkan pada tingkat provinsi memiliki fungsi-fungsi seperti pendaftaran haji plus, validasi atau pemeriksaan dokumen haji, pembatalan haji, *monitoring* (jumlah jemaah haji, jumlah pendaftaran calon jemaah haji perhari). SISKOHAT sudah mencakupi seluruh tugas pokok dari kelima seksi dari bidang penyelenggaraan haji dan umrah. Adapun seksi-seksi tersebut adalah seksi SISKOHAT, seksi Pendaftaran dan Dokumen Haji, seksi Pembinaan Haji dan Umrah, seksi Pengelolaan Keuangan Haji, seksi Akomodasi, Transportasi, dan Perlengkapan Haji.

Pada tingkat provinsi, pendaftaran haji ditujukan untuk pendaftaran haji khusus. Sedangkan, pendaftaran haji reguler dilakukan oleh Kemenag Kab/Kota. Berikut ini adalah proses bisnis dari SISKOHAT dalam alur proses pendaftaran haji khusus:

1. Calon Jemaah haji membuka rekening tabungan haji pada BPS BPIH.
2. Pengajuan permohonan SPPH ke *travel agent* dengan mengisi formulir SPPH. Adapun syarat-syaratnya adalah:
    a. Surat Keterangan sehat dari dokter
    b. *Fotocopy* KTP dan Kartu Keluarga
    c. *Fotocopy* Akte Kelahiran/ Surat Nikah/ Ijazah
    d. *Fotocopy* buku tabungan
    e. Pas foto terbaru sebanyak 10 lembar dengan latar foto berwarna putih.
3. Pihak *Travel agent* melakukan permohonan SPPH ke kanwil Kemenag Provinsi.
4. Pegawai Kanwil Kemenag Provinsi melakukan pengisian data calon jemaah ke dalam SISKOHAT Gen 2.
5. Dari SISKOHAT Gen 2, akan diperoleh nomor pendaftaran SPPH.

6. *Travel agent* membawa nomor SPPH tersebut ke BPS BPIH dan membayar setoran awal.
7. BPS BPIH melakukan transfer setoran.
8. BPS BPIH memasukkan nomor pendaftaran SPPH.
9. Data pembayaran tersebut secara terintegrasi akan masuk ke dalam database SISKOHAT, dan mendapatkan nomor porsi.
10. Setelah transaksi pembayaran berhasil, maka calon jemaah mendapatkan bukti setor BPIH sebanyak 5 lembar.
    a. Lembar pertama (asli) untuk jemaah haji.
    b. Lembar kedua untuk BPS BPIH.
    c. Lembar ketiga untuk PIHK.
    d. Lembar keempat untuk Kanwil Kemenag Provinsi.
    e. Lembar kelima untuk direktorat pelayanan Jenderal penyelenggaraan Haji dan Umrah pusat.
11. Calon jemaah melaporkan bukti setor lembar ke 2, 3 dan 4 (kuning, biru, merah).
12. Pegawai melakukan pemeriksaan dan validitas data melalui menu *monitoring* pembayaran.
13. Pegawai memasukkan nomor porsi.
14. Calon jemaah haji telah terdaftar.

Secara lebih jelas, berikut ini alur proses pendaftaran haji secara singkat dapat digambarkan sebagaimana berikut:



Gambar 4.2. Proses Pendaftaran Haji Khusus

Secara keseluruhan, proses bisnis yang dilakukan pegawai dalam menggunakan SISKOHAT Gen 2 yaitu:

1. Pengguna memasukkan url *Virtual Private Number* (VPN) SISKOHAT Gen 2. Kemudian melakukan *log in* dengan *user ID dan Password.*
2. Jika berhasil *log in*, maka halaman utama sistem akan tampil. Jika gagal, maka akan kembali ke halaman *log in*.
3. Memilih menu *entry* SPPH.
4. Pegawai memasukkan data-data calon jemaah haji.
5. Klik *button* simpan, untuk menyimpan data ke *database*.
6. Klik *button* cetak untuk mencetak formulir SPPH.
7. Memberikan nomor SPPH kepada calon jemaah untuk selanjutnya melakukan pembayaran.
8. Calon jemaah melaporkan bukti setor dari BPS BPIH.
9. Pegawai mengecek melalui menu *monitoring*.
10. Pegawai mengklik sub menu *monitoring* SPPH Pendaftaran.
11. Pegawai memasukkan nomor porsi.
12. Muncul tampilan data calon jemaah yang sudah terdaftar.

13. Pegawai memilih menu informasi, lalu sub menu informasi *waiting list* jemaah haji.
14. Pegawai memberitahu estimasi keberangkatan kepada calon jemaah haji.

Pendaftaran haji merupakan proses bisnis utama dalam bidang penyelenggaraan haji dan umrah. Adapun rincian dan aliran data pendaftaran haji yang dihasilkan adalah:

1. Kementrian agama kabupaten/kota
    a. Surat rekomendasi penerbitan paspor.
    b. Surat pengantar pengiriman paspor ke Kanwil.
    c. Paspor jemaah haji.
    d. Bukti setoran lunas BPIH lembar ke 2.
    e. Daftar nominatif daerah tingkat II.
2. Kanwil Kemenag Provinsi
    a. Surat pengantar pengiriman paspor ke pusat.
    b. Paspor jemaah haji.
    c. Bukti setoran lunas BPIH lembar ke-2.
    d. Daftar nominatif provinsi.
    e. Surat tugas.
    f. SPD.
3. Kesekretariatan
    a. administrasi penerimaan & penyerahan paspor.
    b. perhitungan paspor.
    c. Pengarsipan.
    d. Pelaporan.
4. Penelitian
    a. Pencocokan data secara manual maupun sistem, meliputi:
        1) Data identitas & foto calon jemaah haji di paspor, setoran awal, daftar nominatif provinsi, maupun lembar setoran lunas.
        2) Masa berlaku paspor & jumlah halaman paspor.
    b. Pemberian nomor nominatif pusat secara fisik pada *cover*/sampul belakang paspor.
5. *Scanning*

a. *scanning fullpage* bukti setoran lunas BPIH lembar ke-2.
b. *scanning* paspor dengan alat MRTD.

6. Pemaduan Data
   a. pemaduan data dan foto calon jemaah haji:
      1) Data sistem dengan data paspor.
      2) Foto sistem dengan foto paspor.
   b. Pemberian nomor nominatif pada sistem sesuai dengan stiker nominatif pusat.
7. *Request* visa
   a. Pengisian formulir permohonan visa melalui SISKOHAT atau dengan mengisi formulir melalui website Kementrian Luar Negeri Arab Saudi.
   b. Pencetakan stiker *barcode* nominatif hasil pemaduan.
8. KBAS & Konfirmasi Visa
   a. Proses pengiriman paspor ke KBAS untuk diterbitkan visa.
   b. Konfirmasi visa calon jemaah haji ke dalam sistem.
   c. Pencetakan manifest tanda terima penyerahan paspor yang telah di devisa.
9. Kanwil Kemenag Provinsi
   a. Menerima paspor yang sudah di visa setelah diteliti dan kebenaran visa calon jemaah haji.
   b. Menyerahkan paspor yang sudah di visa ke masing-masing kemenag kab/kota.
10. Kemenag Kab/Kota

    Menyerahkan paspor ke calon jemaah haji.

4.1.2.2.Identifikasi Aset Kritis

Hasil analisa proses bisnis yang telah dilakukan terdapat aset kritis yang perlu dilakukan pengukuran risiko. Berikut ini adalah daftar dari aset kritis yang dikategorisasikan berdasarkan *hardware, software, people, data,* dan *network* (Desy et al., 2014). Deskripsi dari aset kritis diperoleh dari hasil wawancara yang telah dilakukan terkait aset kritis TI pada Bidang Penyelenggaraan Haji dan Umrah.

Tabel 4.2. Daftar Aset Kritis TI

Kategori Aset	Aset Kritis	Deskripsi
Hardware	*Server*	Menyimpan data-data yang ada pada SISKOHAT.
	Komputer/PC	Perangkat komputer yang digunakan untuk melakukan pengolahan data jemaah haji yang hanya dapat diakses pada komputer instansi di Bidang Penyelenggaraan Haji dan Umrah.
	Perangkat jaringan Internet dan intranet.	Perangkat jaringan yang digunakan sebagai pendukung agar SISKOHAT dapat diakses dan digunakan.
	Printer/ scanner	Alat pendukung untuk mencetak laporan, data jemaah haji ataupun data lainnya.
Software	Antivirus	Antivirus yang digunakan adalah AVAST dan AVG. *Software* pada PC untuk mendeteksi serta mencegah virus yang masuk pada komputer.
	Sistem Operasi PC/*Server*	Digunakan sebagai *software* untuk mendukung sistem ini di bagian sistem operasi.
	JRE (Java Runtime environment)	Aplikasi agar data foto *fingerprint* dan foto calon jemaah dapat terlihat pada sistem.
	Microsoft Office	Aplikasi pendukung dalam kegiatan proses bisnis pada bidang penyelenggaraan haji dan umrah.
People	Kepala Bidang Penyelenggaraan Haji dan Umrah	*Monitoring* data-data jemaah haji (laporan)
	KASI Sistem Komputerisasi Haji	*Monitoring* data jemaah haji dan umrah, dan menginformasikan

	Terpadu	perubahan-perubahan modul ataupun yang berkaitan dengan sistem, dan informasi jemaah haji.
	KASI Pembinaan Haji dan Umrah	*Monitoring* data Pembimbing haji dan umrah.
	KASI Pendaftaran dan Dokumen Haji	*Monitoring* data dan dokumen haji (verifikasi dokumen)
	KASI Pengelolaan Keuangan Haji	*Monitoring* data keuangaan haji.
	KASI Akomodasi, Transportasi, dan Perlengkapan Haji.	*Monitoring* perlengkapan dan kebutuhan haji.
	Staff Haji dan Operator SISKOHAT	Menjalankan tugas pembatalan dan pendaftaran haji.
Data	Data Jemaah Haji (Reguler dan Khusus)	Biodata dari calon jemaah haji dan umrah yang terdaftar.
	Data Jadwal Keberangkatan	Informasi keberangkatan jemaah haji setiap tahun.
	Data Nomor Porsi	Informasi nomor porsi ataupun estimasi keberangkatan calon jemaah haji.
	Data Pembatalan Jemaah Haji	Informasi biodata jemaah haji yang batal berangkat ataupun tertunda.
	Data Keuangan setelah audit	Informasi kas haji setelah dilakukan audit.
	Data Travel	Informasi terkait data travel agent yang memiliki izin operasi.
	Data Petugas Haji	Informasi terkait data petugas haji yang bertugas atau sebagai pembimbing haji.
	Data KBIH	Data kelompok bimbingan ibadah haji.
Network	Internet	Jaringan yang dimanfaatkan oleh pihak instansi untuk saling bertukar

		data dan informasi secara meluas, tidak hanya dalam lingkungan instansi namun juga di luar lingkungan instansi. SISKOHAT diakses pada lapisan *end user* (calon jemaah) dapat dilakukan dengan jaringan internet.
	Intranet	Jaringan pribadi atau jaringan komputer yang digunakan oleh instansi untuk berbagi data dan informasi rahasia instansi kepada pegawainya. Dalam hal ini menggunakan jaringan VPN.

Sumber: Olahan Peneliti, 2018

4.1.2.2.Profil Aset Berbasis Ancaman

Profil aset berbasis ancaman disusun berdasarkan pendefinisian profil kebutuhan keamanan, ancaman, praktik keamanan sekarang, dan kelemahan organisasi sekarang. Masing-masing aspek tersebut akan dijabarkan sebagai berikut:

A. Profil kebutuhan keamanan

Dalam OCTAVE, untuk melindungi aset kritis dilakukan pendefinisian hal-hal apa saja penting pada masing-masing aset. Selanjutnya dapat ditentukan pengembangan apa saja yang dibutuhkan untuk melindungi aset tersebut (Alberts & Dorofee, 2002). Profil kebutuhan keamanan Teknologi Informasi dibangun berdasarkan aspek keamanan informasi yaitu *Confidentiality*, *Integrity*, dan *Availability*(Whitman & Mattord, 2012), (Alberts & Dorofee, 2002). Pendefinisian kebutuhan ini berdasarkan hasil observasi lapangan dan wawancara yang telah dilakukan.

Tabel 4.3. Profil KebutuhanKeamanan

Aset Kritis	***Confidentiality***	***Integrity***	***Availability***
		Hardware	
Server	Harus dijamin kredibilitas serta kepastian sistem terhadap pengguna yang berhak	Harus dijaga keberadaannya dari orang yang tidak berhak baik secara fisik dan logika	*Hardware* harus bisa digunakan secara optimal selama 24 jam 7 hari
Komputer/PC	Harus dijamin kerahasiaan *log in* pada komputer yang digunakan	Tidak boleh ada yang bisa *log in* ke sistem kecuali orang yang berhak	Perangkat komputer harus bisa berfungsi selama jam kerja
Perangkat jaringan internet, intranet	Letak perangkat jaringan harus diletakkan diluar jaungkauan pihak yang tidak berwenang	Konfigurasi jaringan hanya boleh dilakukan oleh administrator.	Harus dapat menyambungkan berbagai koneksi internet dan data ke *server* dan jaringan luar maupun lokal.
Printer/ scanner	Dipergunakan seoptimal mungkin oleh pihak yang berwenang.	Hanya orang yang berkepentingan saja yang dapat menggunakan perangkat.	Harus dapat berfungsi selama jam kerja.
		Software	
Antivirus	Yang berhak mengganti atau melakukan *upgradesoftware* hanya teknisi atau operator.	Antivirus yang digunakan tidak boleh meyerang data-data penting perusahaan	Antivirus dapat mendeteksi serangan virus kapanpun.
Sistem Operasi PC/*Server*	Tidak boleh diakses oleh pihak yang tidak berwenang	Tidak boleh mengganti sistem operasi tanpa izin.	Sistem operasi harus dapat digunakan selama jam kerja

			berlangsung.
JRE Microsoft Office	Yang berhak mengganti atau melakukan *upgradesoftware* hanya teknisi atau operator.	Tidak boleh mengganti atau menghapus *software* ini tanpa izin.	Dapat digunakan selama jam kerja berlangsung.
People			
Kepala Bidang Penyelenggaraan Haji dan Umrah KASI Sistem Komputerisasi Haji Terpadu KASI Pembinaan Haji dan Umrah KASI Pendaftaran dan Dokumen Haji KASI Pengelolaan Keuangan Haji KASI Akomodasi, Transportasi, dan Perlengkapan Haji.	Melihat laporan pada sistem sesuai dengan hak akses.	Tidak dapat merubah dan menghapus data calon jemaah haji.	*Monitoring* dapat dilakukan selama jam kerja.
Staff Haji dan Operator SISKOHAT	Pegawai yang akan menggunakan sistem harus mendapatkan pelatihan terlebih dahulu.	Tidak adanya pemalsuan dan kesalahan dalam penginputan data calon jemaah haji.	Harus siap melayani ketersediaan sistem selama 24 jam dan 7 hari.
Data			
Data Jemaah Haji (Reguler dan Khusus) Data Pembatalan	Tidak boleh dilihat oleh orang yang tidak memiliki hak otorisasi karena data	Tidak bisa memodifikasi data-data yang telah diinputkan. Dan data	Data dapat diakses ketika dibutuhkan.

Jemaah Haji Data Keuangan setelah audit	tersebut bersifat rahasia.	tidak boleh diambil oleh orang yang tidak berwenang.	
Data Nomor Porsi Data Jadwal Keberangkatan	Hanya bisa dilakukan pengecekan oleh pihak kemenag (operator) pada SISKOHAT Kemenag, dan calon jemaah haji (pemilik nomor porsi) yang diakses pada situs Kemenag.	Hanya fungsi view, tidak dapat memodifikasi data.	Data dapat diakses 24 jam 7 hari.
Network			
Internet	Pihak yang *log in* ke sistem harus dilindungi kerahasiaan autentikasinya.	Tidak boleh ada yang bisa *log in* ke sistem kecuali orang yang berhak.	Jaringan tersedia selama 24 jam 7 hari.
Intranet	Sambungan jaringan hanya dapat digunakan di perangkat dan lokasi tertentu.	Perangkat yang tidak disetujui tidak boleh disambungkan ke jaringan.	Jaringan dapat digunakan selama jam kerja.

Sumber: Olahan Peneliti, 2014

B. Ancaman terhadap aset kritis

Ancaman aset kritis TI dilihat berdasarkan sumber ancaman internal dan ancaman eksternal(Loch et al., 1992). Ancaman internal merupakan potensi kemungkinan terjadinya serangan yang bersumber dari internal organisasi. Sedangkan ancaman ekternal merupakan potensi kemungkinan terjadinya

serangan yang berasal dari eksternal organisasi. Penyusunan ancaman tersebut juga berdasarkan kondisi dari lapangan dan wawancara yang telah dilakukan. Sedangkan untuk mendefinisikan risiko yang bersumber dari kedua hal tersebut, dilakukan penyusunan ancaman internal dan eksternal dengan melihat kategorisasi ancaman (Whitman & Mattord, 2012). Berikut ini adalah daftar ancaman dari aset kritis:

Tabel 4.4. Ancaman aset kritis

Kategori Aset	**Aset Kritis**	**Ancaman**	
		Internal	**Eksternal**
Hardware	*Server*	- Kebakaran *server* yang mengalami *overheat* - *Server over heat* karena tidak berfungsinya AC pada ruangan - *Server down* karena terlalu banyaknya unit yang mengakses *server* pada waktu bersamaan. - *Server* rusak karena Tidak adanya proses *controlling* dan *maintenance* secara rutin sehingga menyebabkan penurunan kinerja dan kerusakan pada *server*.	- Terjadinya bencana alam seperti banjir, kebakaran, tersambar petir. (*Force of nature*) - *Server* rusak karena terkena reruntuhan bangunan (*server* terletak di lantai bawah)
	Komputer/PC	- Kesalahan dalam	- Terjadinya bencana

		konfigurasi komputer sehingga tidak dapat digunakan - Adanya serangan virus pada PC yang menyebabkan PC menjadi rusak - Lisensi *software* yang digunakan sudah melebihi batas waktu	alam seperti banjir, kebakaran, tersambar petir. (*Force of nature*) - Hilangnya komponen PC karena pencurian. - Pencurian hak akses PC karena adanya pihak yang tidak bertanggungjawab mencuri informasi hak akses PC untuk dapat mengakses PC.
	Perangkat jaringan internet, intranet	- Kerusakan pada infrastruktur jaringan seperti *switch/hub*, *router, access point*. - Manipulasi konfigurasi jaringan.	- Terjadinya bencana alam seperti banjir, kebakaran, tersambar petir. (*Force of nature*) - Hilangnya komponen perangkat jaringan karena pencurian. - Kabel jaringan digigit tikus.
	Printer/ scanner	- Rusaknya *printer/ scanner* karena *maintenance* dan kontrol yang tidak rutin.	- Terjadinya bencana alam seperti banjir, kebakaran, tersambar petir. (*Force of nature*) - Hilangnya *printer/ scanner* karena pencurian.
Software	Antivirus	- Lisensi *software* yang	- Terjadinya bencana

	Sistem Operasi PC/*Server* Java Microsoft Office	digunakan sudah melebihi batas waktu - Serangan virus karena Antivirus tidak mampu mendeteksi dan mencegah virus yang masuk	alam seperti banjir, kebakaran, tersambar petir. (*Force of nature*)
People	Kabid Penyelenggaraan Haji dan Umrah KASI Sistem Komputerisasi Haji Terpadu KASI Pembinaan Haji dan Umrah KASI Pendaftaran dan Dokumen Haji KASI Pengelolaan Keuangan Haji KASI Akomodasi, Transportasi, dan Perlengkapan Haji. Staff Haji dan Operator SISKOHAT	- Penyalahgunaan hak akses yang dimiliki. - *Human failure*, yaitu kesalahan dalam penginputan data dan penggunaan perangkat sistem. - SDM kurang kompeten	- Adanya kerjasama dengan pihak luar untuk melakukan pemalsuan tanda tangan yang tercatat pada sistem - Pelayanan terhadap calon jemaah haji tidak maksimal.
Data	Data Jemaah Haji (Reguler dan Khusus) Data Jadwal Keberangkatan Data Nomor Porsi Data Pembatalan Jemaah Haji Data Keuangan	- Kurangnya pengontrolan kapasitas memori *server* dan *storage* yang telah terpakai - Penyebaran informasi rahasia oleh pegawai. - Pembobolan informasi terhadap sistem dengan	- Pencurian data atau informasi oleh orang yang tidak berwenang. - Terjadinya bencana alam seperti banjir, kebakaran, tersambar petir. (*Force of nature*)

	setelah audit Data Travel Data Petugas Haji Data KBIH	melakukan berbagi *password*. - Ketidakcocokan antara data pada sistem dengan data fisik. - Hilangnya data karena *software failure.* - Kurangnya keamanan pada sistem (*firewall*) - Data korup karena jaringan internet yang kurang optimal. - Data tidak dapat diakses (sistem error)	
Network	Internet Intranet	- Jaringan LANtidak cepat - Konektivitas internet yang menurun - Adanya koneksi terputus - Adanya kesalahan pengalamatan IP	- Penyadapan informasi penting melalui jaringan seperti celah masuknya *hacker* dan *Remote Spying*. - Rusaknya kabel jaringan karena digigit tikus, atau pihak eksternal mengubah posisi kabel.

Sumber: Olahan Peneliti, 2018

C. Keamanan yang sudah diterapkan

Berdasarkan hasil wawancara dan observasi lapangan yang telah dilakukan, berikut ini adalah keamanan yang sudah diterapkan pada bidang ini:

1. Pemantauan ruangan melalui CCTV

Penerapan keamanan dilakukan dengan pemasangan perangkat CCTV untuk memantau keadaan ruangan yang terdapat aset kritis teknologi informasi. CCTV dipasang pada sudut-sudut atas ruangan yang dapat melihat pergerakan keluar dan masuknya orang-orang dari ruangan. CCTV bertujuan juga untuk

menjaga aset dari pencurian perangkat, ataupun merekam segala kejadian yang terjadi pada ruangan tersebut.

2. Penggunaan sekat atau pembatas ruangan

Dahulunya ruangan SISKOHAT terdiri satu ruangan yang bebas, dan dilantai atas dikhususkan untuk seksi SISKOHAT. Akan tetapi, pengaturan tersebut masih dirasa kurang aman bagi pihak Kementerian Agama Provinsi Riau. Sehingga, kondisi ruangan dirubah dengan memberikan sekat-sekat ruangan untuk menghindari bebasnya tamu yang masuk. Sekat pada lantai dasar dilakukan dengan memberikan partisi bagi ruangan Kepala Bidang Penyelenggaraan Haji dan Umrah, partisi bagi ruangan pegawai internal termasuk ruangan para KASI. Kemudian, di lantai atas terdapat ruangan bagi Seksi Keuangan Haji. Sehingga, bagi para tamu (calon jemaah) yang ingin mendapatkan informasi akan mendatangi *counter desk operator* yang ditemui saat memasuki ruangan Bidang Penyelenggaraan Haji dan Umrah. Dengan demikian, pengawasan dan kontrol terhadap orang-orang yang tidak berkepentingan dapat dilakukan lebih baik.

3. Pengingat untuk mematikan perangkat TI

Setiap hari pada saat jam kerja habis yaitu sekitar pukul 16.00 WIB, terdapat pengumuman yang diperuntukkan bagi seluruh pegawai. Pengumuman berguna untuk mengingatkan pegawai agar mematikan seluruh perangkat komputer, mematikan lampu serta AC. Kemudian, *cleaning service* akan melakukan pengecekan ruangan, membersihkan ruangan, dan mengunci ruangan.

4. Jalur masuk satu pintu

Kementerian Agama menerapkan jalur masuk satu pintu dan keluar satu pintu. Hal ini dimaksudkan agar satpam dapat melakukan pengawasan orang-orang yang masuk ke dalam wilayah kantor Kementerian Agama Provinsi Riau. Sehingga, sebagai tamu harus wajib lapor dan memberitahukan kepentingannya kepada satpam. Selanjutnya, satpam akan memberikan arahan dan petunjuk kepada tamu.

5. Penggunaan jaringanVPN (*Virtual Private Network*)

SISKOHAT hanya dapat diakses menggunakan link VPN (Virtual Private Network) jaringan pribadi (bukan untuk akses umum) yang menggunakan medium nonpribadi (misalnya internet) untuk menghubungkan antar *remote-site*secara aman. Hanya Kepala Bidang, Kepala Seksi dan staff pada bidang penyelenggaraan haji dan umrah saja yang mengetahui alamat VPN tersebut. Dan alamat VPN antara KASI dan Staf juga berbeda, sehingga tingkat keamanan lebih tinggi.VPN dapat diakses oleh orang-orang yang telah memiliki wewenang (*username* dan *password*) untuk dapat masuk ke jaringannya. Setelah berhasil masuk jaringan, maka akan masuk ke halaman *log in* SISKOHAT. Kemudian, SISKOHAT dapat diakses dengan memasukkkan *username* dan *password*yang telah dimiliki. Jika terjadi tiga kali kesalahan dalam *log in,* maka akun akan diblokir. Sehingga, pengurusannya dilakukan dengan melakukan koordinasi kepada Kemenag Pusat untuk mendapatkan akun kembali ataupun *reset password*.

6. Kondisi lingkungan

Gedung Kanwil Kemenag Riau merupakan kepemilikan pemerintah. Gedung berada di tengah kota Pekanbaru dan terletak pada jalur protokol kota Pekanbaru. Kanwil Kemenag Riau belum pernah mengalami kebakaran, kejatuhan pesawat, banjir, angin topan, gempa bumi, gunung meletus, tsunami, pencurian, huru-hara, fluktuasi tegangan, tertabrak mobil, dan tertimpa pohon. Bidang Penyelenggara haji dan umrah memiliki ruangan yang luas dan struktur bangunan yang kuat dan kokoh. Gedung Bidang Penyelenggaraan Haji dan Umrah ini terdiri dari dua lantai bertingkat dengan tangga. Lantai bawah merupakan operator melayani calon jemaah yang ingin mendapatkan informasi haji, atau mengumpulkan dokumen, serta terdapat ruangan pegawai dan ruangan Kepala Bidang. Sedangkan lantai atas merupakan ruang Seksi Keuangan Haji.*Server* terletak pada gedung yang terpisah, yaitu dibagian Bidang Informasi Masyarakat (Inmas) berada pada lantai dasar.

7. Pembatasan hak akses

Pada Bidang Penyelenggaraan Haji dan Umrah tingkat Provinisi hanya bisa melakukan input data dan *monitoring* data (*view*). Sedangkan menuedit dan hapus dilakukan oleh Kanwil Kemenag RI. Sehingga, jika terjadi kesalahan penginputan data ataupun proses pembatalan calon jemaah haji, dilakukan dengan koordinasi dengan pihak pusat untuk perbaikan data. Hal ini dilakukan sebagai upaya kecermatan dalam penginputan data dan menghindari modifikasi data oleh orang yang tidak berwenang ataupun penyalahgunaan hak akses.

8. Penggantian *password*

Penggantian *password* dilakukan oleh Kanwil Kemenag RI, dan secara rutin penggantian *password* minimal dilakukan 1 kali dalam setahun. Adapun pengeditan akun juga dilakukan dengan meminta persetujuan dan dilakukan oleh Kemenag RI.

D. Kelemahan organisasi

Berdasarkan hasil observasi dan wawancara yang telah dilakukan, maka kelemahan organisasi yang diidentifikasi adalah:

1. *Server* pusat SISKOHAT ada di Jakarta, sehingga apabila *server* di Jakarta mengalami masalah seperti *server down* maka dapat mempengaruhi jaringan pengiriman data di Kanwil Kemenag Provinsi Riau.
2. Tata letak *server* Kanwil Kemenag Provinsi Riau berada pada lantai dasar. Sehingga, terancam mengalami bencana alam seperti keruntuhan bangunan, banjir, dan sebagainya.
3. Masih kurangnya kesadaran instansi terhadap risiko TI. Seperti penjagaan *password* dan *username*, masih terdapat pegawai yang menempelkan *password* dan *username* pada monitor ataupun di atas meja. Sehingga, kerahasiaan akun ataupun hak akses sistem terancam.
4. Dari segi *maintenance hardware* dilakukan secara menyeluruh (Kanwil Kemenag Riau) satu kali dalam setahun yang dilakukan oleh tim dari Kementerian Agama RI. Akan tetapi, hanya *monitoring* dan tidak detail kepada *maintenance* di Bidang Penyelenggaraan Haji dan Umrah. Sedangnya

maintenance hardware di *monitoring* oleh pihak Kementerian Agama Provinsi Riau setiap satu kali 6 bulan. Belum terdapat dokumentasi *maintenance* yang dilakukan secara prosedural.

5. Tidak ada UPS ataupun *Genset*. Sehingga tidak adanya penanganan jika lampu mati ataupun tidak cukupnya daya listrik.
6. Belum adanya identifikasi risiko di pada Bidang Penyelenggaraan Haji dan Umrah dalam penggunaan SISKOHAT, sehingga menanganan risiko hanya dilakukan ketika masalah itu terjadi.
7. Belum adanya dokumen yang jelas (user manual) yang detail mengenai penggunaan SISKOHAT.
8. Pelatihan pegawai masih kurang yang dikirimkan sekali dalam setahun. Delegasi tiap provinsi mengutus satu orang untuk mengikuti pelatihan tersebut.

4.1.2.3.Identifikasi Kelemahan Infrastruktur

Berikut ini penjelasan dari identifikasi kelemahan infrastruktur yang ada pada Bidang Penyelenggaraan Haji dan Umrah Kantor Wilayah Kementerian Agama Provinsi Riau.

A. Komponen Utama

Komponen utama menjelaskan mengenai penggunaan infrastruktur dan informasi yang ada pada Bidang Penyelenggaraan Haji dan Umrah sebagai bagian dari proteksi aset TI yang digunakan, yang dijelaskan sebagai berikut :

1. *Server* di dalam Kanwil Kemenag Provinsi Riau terdapat *server* dengan data akan langsung terhubung ke dalam *server* pusat di Jakarta.
2. Jaringan yang digunakan menggunakan VPN untuk mengakses SISKOHAT. Jaringan berupa internet dan intranet.
3. Perangkat PC dan *Printer/ scanner* sebagai perangkat yang digunakan dalam mengakses SISKOHAT, serta perangkat keras yang digunakan mendukung proses bisnis yang ada pada instansi.
4. Antivirus digunakan untuk mendukung *maintenance* dari setiap *software* dan sistem operasi, yang berfungsi untuk *update* agar meminimalisir virus yang mengancam.

5. *Software* JRE sebagai *software*yang dapat menampilkan data foto *fingerprint* dan foto calon jemaah haji.
6. Sistem Operasi yang digunakan bagi pengguna adalahsistem operasi *Windows 7* ataupun *Windows 10*. Akan tetapi, SISKOHAT lebih *compatible* dengan *Windows 7*.
7. *People* yaitu sumber daya manusia yang mengakses SISKOHAT yaitu para pegawai Bidang Penyelenggaraan Haji dan Umrah.

B. Kerentanan Teknologi Saat Ini

Setelah diperoleh data komponen kunci selanjutnya dilakukan evaluasi terhadap kerentanan komponen kunci tersebut.

Tabel 4.5. Kerentanan Teknologi Saat Ini

Komponen Utama	Kerentanan
Server	1. *Server* pusat SISKOHAT ada di Jakarta, sehingga apabila *server* di Jakarta mengalami masalah seperti *server down* maka dapat mempengaruhi jaringan pengiriman data di Kanwil Kemenag Provinsi Riau. 2. Tata letak *server* Kanwil Kemenag Provinsi Riau berada pada lantai dasar. Sehingga, terancam mengalami bencana alam seperti keruntuhan bangunan, banjir, dan sebagainya. 3. Serangan DDOS yaitu serangan yang biasanya terjadi pada *server* dilakukan melalui jaringan internet sehingga mengacaukan sistem kerja *server*.
Jaringan	Terputusnya koneksi karena jaringan tidak dapat digunakan akibat rusaknya kabel jaringan, serangan *hacker*, ataupun permasalahan *bandwidth.*
PC	Serangan virus yang dapat merusak data-data penting yang ada pada PC.
Antivirus	*Software* tidak dapat melakukan *update* secara otomatis
JRE	*Software* tidak dapat berfungsi dan menampilkan data foto *fingerprint* dan foto dari calon jemaah haji.
Sistem Operasi	*Software* masih terdapat celah keamanan, seperti penggunaan

	sistem operasi yang tidak berlisensi. Apabila tidak menggunakan sistem operasi resmi maka apabila terjadi kerusakan dapat menyebabkan sistem operasi tidak berfungsi dan tidak dapat digunakan.
Sistem (SISKOHAT)	Masih terdapatnya celah keamanan. Terdapat kegagalan sistem, kelemahan keamanan.
People	*Social engineering* yang menyebabkan kebocoran data ataupun informasi penting oleh pihak internal kepada pihak eksternal/pihak yang tidak bertanggungjawab.

Sumber: Olahan Peneliti, 2018

4.1.3. Analisis Risiko

Penyusunan daftar risiko dilakukan berdasarkan hasil dari identifikasi proses bisnis dan aset kritis yang telah dilakukan. Kemudian, membangun profil berbasis ancaman sesuai dengan tahapan pada OCTAVE untuk mendifinisikan risiko (Alberts & Dorofee, 2002). Adapun tabel FMEA yang digunakan sebagai acuan adalah tabel FMEA dari *American Society for Quality* (ASQ) yang digunakan dan disesuaikan dengan ISO 27001 (Security, 2008).

4.1.3.1.Hasil Analisis Risiko Tim 1

Penilaian risiko dilakukan berdasarkan daftar risiko yang telah diverifikasi dan divalidasi oleh tim. Sebelum melakukan penilaian, koordinator tim memberikan penjelasan terkait tata cara pengisian dari nilai parameter FMEA. Tim pertama terdiri dari dua orang fasilitator dan kepala seksi SISKOHAT. Kepala Seksi SISKOHAT menjadi informan yang menjadi sumber informasi dalam melakukan pengisian nilai masing-masing parameter. Sedangkan, fungsi dari praktisi TI menanyakan daftar risiko dan menggali informasi dari informan. Kemudian, fungsi dari koordinator adalah memimpin proses diskusi. Dalam pemberian nilai, fasilitator dan kepala seksi berdiskusi untuk mengetahui skala kriteria yang tepat untuk menjawab masing-masing daftar risiko. Berikut ini adalah hasil dari penilaian risiko dari tim pertama:

Tabel 4. 6. Hasil Penilaian Tim 1

Code	*Process Function (Category)*	*Critical Assets*	*Potential Failure Modes (process defects)*	*Potential Effect(s) of Failure*	*SEV*	*Potential Cause(s) of Failure*	*OCC*	*Current Process Controls*	*DET*	*RPN*
HW01	*Hardware*	*Server*	Kebakaran *Server*	Kegiatan operasional ataupun kinerja terhenti	3	*Server* mengalami *overheat*	1	Melakukan pengecekan ruangan *server* setiap hari.	10	30
HW02			Kebakaran *Server*	Kerugian Finansial	6	Hubungan arus pendek (*power failure*)	1	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	10	60
HW03			*Serveroverheat*	Kegiatan operasional ataupun kinerja terhambat	3	Tidak berfungsinya AC pada ruangan *server*	4	Melakukan pengecekan ruangan *server* setiap hari.	5	60
HW04			*Server* down	Kegiatan operasional ataupun kinerja terhambat	6	Terlalu banyaknya unit yang mengakses *server* pada waktu bersamaan ataupun serangan DDOS.	9	Melakukan pengecekkan terhadap infrastruktur TI yang rusak.	7	378
HW05			Kerusakan *server*	*Server* tidak dapat digunakan	6	Tidak adanya proses *controlling* dan *maintenance* secara rutin	4	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	6	144
HW06			Kerusakan *server*	Kerugian finansial	2	Bencana alam seperti terkena reruntuhan bangunan (*server* terletak di lantai bawah)	4	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	8	64
HW07		Komputer/ PC	Kerusakan Komputer	Kegiatan operasional ataupun kinerja terhambat	7	Adanya serangan virus	4	Adanya antivirus setiap PC	1	28
HW08			Komputer tidak dapat digunakan	Kegiatan operasional ataupun kinerja terhambat	6	Kesalahan dalam konfigurasi komputer	2	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	5	60
HW09			Komputer tidak dapat digunakan	Kegiatan operasional ataupun kinerja terhambat	3	Lisensi *software* yang digunakan sudah melebihi	1	Melakukan pengecekkan terhadap infrastruktur TI	5	15

Code	*Process Function (Category)*	*Critical Assets*	*Potential Failure Modes (process defects)*	*Potential Effect(s) of Failure*	*SEV*	*Potential Cause(s) of Failure*	*OCC*	*Current Process Controls*	*DET*	*RPN*
						batas waktu		yang rusak		
HW10			Komputer tidak dapat digunakan	Kerugian finansial	7	Bencana alam (kebakaran, banjir, petir)	2	Melakukan pengecekkan terhadap infrastruktur TI yang rusak, mematikan perangkat sebelum pulang.	1	14
HW11			Perangkat komputer *out of dated*	Kegiatan operasional ataupun kinerja terhambat	1	Usangnya teknologi yang digunakan	1	*Monitoring* perangkat sekali dalam setahun	1	1
HW12			Hilangnya komponen PC	Kerugian finansial	1	Pencurian	3	Pembatasan dan pengawasan hak akses ruangan, mengunci ruangan dan ada CCTV.	1	3
HW13			Akses informasi PC secara ilegal	Mencuri informasi yang merusak reputasi Instansi	10	Penjagaan hak akses lemah dan atau komputer tidak diberi *password.*	10	Memberikan *password* masing-masing PC pegawai, dan memantau pergerakan yang mencurigakan dari CCTV.	1	100
HW14		Perangkat jaringan	Kegagalan jaringan	Kegiatan operasional ataupun kinerja terhambat	6	Kerusakan pada infrastruktur jaringan seperti *switch/hub*, *router*, *access point*.	4	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	6	144
HW15			Kegagalan jaringan	Kegiatan operasional ataupun kinerja terhambat	6	Manipulasi konfigurasi jaringan.	2	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	6	72
HW16			Kerusakan Perangkat Jaringan	Kegiatan operasional ataupun kinerja terhambat	6	Bencana alam (*force of nature*) dan atau hewan	3	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	7	126

Code	*Process Function (Category)*	*Critical Assets*	*Potential Failure Modes (process defects)*	*Potential Effect(s) of Failure*	*SEV*	*Potential Cause(s) of Failure*	*OCC*	*Current Process Controls*	*DET*	*RPN*
HW17			Hilangnya komponen perangkat jaringan	Kegiatan operasional ataupun kinerja terhambat	6	Pencurian	2	Pembatasan dan pengawasan hak akses ruangan dan adanya CCTV	1	12
HW18		*Printer/ scanner*	Kerusakan *Printer/ scanner*	Tidak dapat mencetak dan melakukan scan data	1	*Maintenance* dan kontrol yang tidak rutin.	6	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	8	48
HW19			Kerusakan *Printer/ scanner*	Tidak dapat mencetak dan melakukan scan data	1	Terjadinya bencana alam seperti banjir, kebakaran, tersambar petir. (*Force of nature*)	1	Melakukan pengecekkan terhadap infrastruktur TI yang rusak, mematikan perangkat sebelum pulang.	1	1
HW20			Hilangnya *printer/ scanner*	Kerugian finansial	1	Pencurian	2	Pembatasan dan pengawasan hak akses ruangan, mengunci ruangan.	1	2
SW01	*Software*	Antivirus, Sistem Operasi, JRE, Ms.Office	Kegagalan *Software*	Kegiatan operasional ataupun kinerja terhambat	6	Lisensi *software* yang digunakan sudah melebihi batas waktu	4	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	2	48
SW02			Serangan Virus	Kegiatan operasional ataupun kinerja terhambat	6	Antivirus tidak mampu mendeteksi dan mencegah virus yang masuk	6	Melakukan update antivirus	1	36
SW03		Sistem (SISKOHAT)	Kegagalan sistem	Kegiatan operasional ataupun kinerja terhenti	6	Sistem masih terdapat celah keamanan	1	Maintenance sistem dilakukan oleh pusat	1	6
PP01	*People*	Kepala dan Staff	Kegagalan Manusia (*Human failure*)	Profesionalitas kinerja	4	kesalahan dalam penginputan data dan penggunaan perangkat sistem	3	Pelatihan sekali dalam setahun dan adanya SOP	4	48

Code	*Process Function (Category)*	*Critical Assets*	*Potential Failure Modes (process defects)*	*Potential Effect(s) of Failure*	*SEV*	*Potential Cause(s) of Failure*	*OCC*	*Current Process Controls*	*DET*	*RPN*
PP02			Kegagalan Manusia (*Human failure*)	Pelayanan terhadap calon jemaah haji tidak maksimal.	4	SDM kurang kompeten	3	Pelatihan sekali dalam setahun	4	48
PP03			Pemalsuan atau penyalahgunaan hak akses	Reputasi intansi	8	Adanya kerjasama dengan pihak luar untuk melakukan pemalsuan tanda tangan yang tercatat pada sistem	1	Tidak adanya hak akses edit ataupun hapus dalam tingkat provinsi.	1	8
DA01	Data	Data	Penuhnya kapasitas	Tidak dapat menyimpan data	6	Kurangnya pengontrolan kapasitas memori *server* dan storage yang telah terpakai	4	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	1	24
DA02			Tersebarnya informasi rahasia	Kerahasiaan data	9	Penyalahgunaan hak akses	2	Adanya aliran data (bertingkat) dalam akses data	1	18
DA03			Pembobolan data/informasi	Kerahasiaan data	10	Penyebaran informasi rahasia oleh pegawai (berbagi *password*)	8	Adanya aliran data (bertingkat) dalam akses data.	1	80
DA04			Tidak cocoknya data pada sistem dengan data fisik	Integritas data	5	Kesalahan operator/pegawai yang menginputkan data	4	Validasi dan verifikasi dokumen	3	60
DA05			Data Hilang	Integritas dan ketersediaan data	10	Kegagalan *software*, jaringan	3	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	1	30
DA06			Cybercrime (hacker attack)	Kerahasiaan, integritas ataupun ketersediaan data terancam	10	Kurangnya keamanan pada sistem (*firewall*)	2	Penggunaan VPN sebagai proteksi jaringan	3	60

Code	*Process Function (Category)*	*Critical Assets*	*Potential Failure Modes (process defects)*	*Potential Effect(s) of Failure*	*SEV*	*Potential Cause(s) of Failure*	*OCC*	*Current Process Controls*	*DET*	*RPN*
DA07			Data Korup	Data tidak dapat diakses ataupun data rusak	10	Jaringan internet yang kurang optimal.	3	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	1	30
NT01	Network	Internet, intranet	Koneksi Jaringan putus	Sistem tidak dapat diakses	6	Kegagalan jaringan	10	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	6	360
NT02			Koneksi Jaringan putus	Sistem tidak dapat diakses	6	Rusaknya perangkat jaringan dan atau mati lampu	6	Melakukan pengecekkan terhadap infrastruktur TI yang rusak, menunggu lampu hidup kembali.	1	36
NT03			Konektivitas jaringan menurun	Sistem error, backup failure, data korup.	6	Kegagalan jaringan	10	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	10	600
NT04			Adanya kesalahan pengalamatan IP	Tidak dapat koneksi jaringan	6	*Human error*	2	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	1	12

4.1.3.2.Hasil Analisis Risiko Tim 2

Penilaian risiko dilakukan berdasarkan daftar risiko yang telah diverifikasi dan divalidasi oleh tim. Sebelum melakukan penilaian, koordinator tim memberikan penjelasan terkait tata cara pengisian dari nilai parameter FMEA. Tim kedua terdiri dari dua orang fasilitator dan operator SISKOHAT. Operator menjadi informan yang menjadi sumber informasi dalam melakukan pengisian nilai masing-masing parameter. Sedangkan, fungsi dari praktisi TI menanyakan daftar risiko dan menggali informasi dari informan. Kemudian, fungsi dari koordinator adalah memimpin proses diskusi.

Dalam pemberian nilai, fasilitator dan operator berdiskusi untuk mengetahui skala kriteria yang tepat untuk menjawab masing-masing daftar risiko. Berikut ini adalah hasil penilaian risiko dari tim kedua:

Tabel 4. 7. Hasil Penilaian Tim 2

Code	*Process Function (Category)*	*Critical Assets*	*Potential Failure Modes (process defects)*	*Potential Effect(s) of Failure*	*SEV*	*Potential Cause(s) of Failure*	*OCC*	*Current Process Controls*	*DET*	*RPN*
HW01	*Hardware*	*Server*	Kebakaran *Server*	Kegiatan operasional ataupun kinerja terhenti	4	*Server* mengalami *overheat*	1	Melakukan pengecekan ruangan *server* setiap hari.	1	4
HW02			Kebakaran *Server*	Kerugian Finansial	1	Hubungan arus pendek (*power failure*)	1	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	1	1
HW03			*Serveroverheat*	Kegiatan operasional ataupun kinerja terhambat	4	Tidak berfungsinya AC pada ruangan *server*	3	Melakukan pengecekan ruangan *server* setiap hari.	1	12
HW04			*Server* down	Kegiatan operasional ataupun kinerja terhambat	7	Terlalu banyaknya unit yang mengakses *server* pada waktu bersamaan ataupun serangan DDOS.	9	Melakukan pengecekkan terhadap infrastruktur TI yang rusak.	7	441
HW05			Kerusakan *server*	*Server* tidak dapat digunakan	7	Tidak adanya proses *controlling* dan *maintenance* secara rutin	4	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	7	196
HW06			Kerusakan *server*	Kerugian finansial	1	Bencana alam seperti terkena reruntuhan bangunan (*server* terletak di lantai bawah)	1	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	1	1
HW07		Komputer/ PC	Kerusakan Komputer	Kegiatan operasional ataupun kinerja terhambat	7	Adanya serangan virus	4	Adanya antivirus setiap PC	1	28
HW08			Komputer tidak dapat digunakan	Kegiatan operasional ataupun kinerja terhambat	6	Kesalahan dalam konfigurasi komputer	2	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	1	12
HW09			Komputer tidak dapat digunakan	Kegiatan operasional ataupun kinerja terhambat	3	Lisensi *software* yang digunakan sudah melebihi	1	Melakukan pengecekkan terhadap infrastruktur TI	3	9

Code	*Process Function (Category)*	*Critical Assets*	*Potential Failure Modes (process defects)*	*Potential Effect(s) of Failure*	*SEV*	*Potential Cause(s) of Failure*	*OCC*	*Current Process Controls*	*DET*	*RPN*
						batas waktu		yang rusak		
HW10			Komputer tidak dapat digunakan	Kerugian finansial	1	Bencana alam (kebakaran, banjir, petir)	1	Melakukan pengecekkan terhadap infrastruktur TI yang rusak, mematikan perangkat sebelum pulang.	1	1
HW11			Perangkat komputer *out of dated*	Kegiatan operasional ataupun kinerja terhambat	1	Usangnya teknologi yang digunakan	1	*Monitoring* perangkat sekali dalam setahun	1	1
HW12			Hilangnya komponen PC	Kerugian finansial	1	Pencurian	1	Pembatasan dan pengawasan hak akses ruangan, mengunci ruangan dan ada CCTV.	1	1
HW13			Akses informasi PC secara ilegal	Mencuri informasi yang merusak reputasi Instansi	10	Penjagaan hak akses lemah dan atau komputer tidak diberi *password.*	10	Memberikan *password* masing-masing PC pegawai, dan memantau pergerakan yang mencurigakan dari CCTV.	3	300
HW14		Perangkat jaringan	Kegagalan jaringan	Kegiatan operasional ataupun kinerja terhambat	6	Kerusakan pada infrastruktur jaringan seperti *switch/hub*, *router*, *access point*.	4	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	3	72
HW15			Kegagalan jaringan	Kegiatan operasional ataupun kinerja terhambat	2	Manipulasi konfigurasi jaringan.	2	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	3	12
HW16			Kerusakan Perangkat Jaringan	Kegiatan operasional ataupun kinerja terhambat	6	Bencana alam (*force of nature*) dan atau hewan	7	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	7	294

Code	*Process Function (Category)*	*Critical Assets*	*Potential Failure Modes (process defects)*	*Potential Effect(s) of Failure*	*SEV*	*Potential Cause(s) of Failure*	*OCC*	*Current Process Controls*	*DET*	*RPN*
HW17			Hilangnya komponen perangkat jaringan	Kegiatan operasional ataupun kinerja terhambat	6	Pencurian	2	Pembatasan dan pengawasan hak akses ruangan dan adanya CCTV	1	12
HW18		*Printer/ scanner*	Kerusakan *Printer/ scanner*	Tidak dapat mencetak dan melakukan scan data	1	*Maintenance* dan kontrol yang tidak rutin.	6	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	6	36
HW19			Kerusakan *Printer/ scanner*	Tidak dapat mencetak dan melakukan scan data	1	Terjadinya bencana alam seperti banjir, kebakaran, tersambar petir. (*Force of nature*)	6	Melakukan pengecekkan terhadap infrastruktur TI yang rusak, mematikan perangkat sebelum pulang.	6	36
HW20			Hilangnya *printer/ scanner*	Kerugian finansial	1	Pencurian	1	Pembatasan dan pengawasan hak akses ruangan, mengunci ruangan.	1	1
SW01	*Software*	Antivirus, Sistem Operasi, JRE, Ms.Office	Kegagalan *Software*	Kegiatan operasional ataupun kinerja terhambat	5	Lisensi *software* yang digunakan sudah melebihi batas waktu	4	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	2	40
SW02			Serangan Virus	Kegiatan operasional ataupun kinerja terhambat	5	Antivirus tidak mampu mendeteksi dan mencegah virus yang masuk	5	Melakukan update antivirus	1	25
SW03		Sistem (SISKOHAT)	Kegagalan sistem	Kegiatan operasional ataupun kinerja terhenti	5	Sistem masih terdapat celah keamanan	1	Maintenance sistem dilakukan oleh pusat	1	5
PP01	*People*	Kepala dan Staff	Kegagalan Manusia (*Human failure*)	Profesionalitas kinerja	5	kesalahan dalam penginputan data dan penggunaan perangkat sistem	3	Pelatihan sekali dalam setahun dan adanya SOP	3	45

Code	*Process Function (Category)*	*Critical Assets*	*Potential Failure Modes (process defects)*	*Potential Effect(s) of Failure*	*SEV*	*Potential Cause(s) of Failure*	*OCC*	*Current Process Controls*	*DET*	*RPN*
PP02			Kegagalan Manusia (*Human failure*)	Pelayanan terhadap calon jemaah haji tidak maksimal.	4	SDM kurang kompeten	3	Pelatihan sekali dalam setahun	4	48
PP03			Pemalsuan atau penyalahgunaan hak akses	Reputasi intansi	9	Adanya kerjasama dengan pihak luar untuk melakukan pemalsuan tanda tangan yang tercatat pada sistem	2	Tidak adanya hak akses edit ataupun hapus dalam tingkat provinsi.	2	36
DA01	Data	Data	Penuhnya kapasitas	Tidak dapat menyimpan data	5	Kurangnya pengontrolan kapasitas memori *server* dan storage yang telah terpakai	5	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	2	50
DA02			Tersebarnya informasi rahasia	Kerahasiaan data	10	Penyalahgunaan hak akses	2	Adanya aliran data (bertingkat) dalam akses data	3	60
DA03			Pembobolan data/informasi	Kerahasiaan data	10	Penyebaran informasi rahasia oleh pegawai (berbagi *password*)	9	Adanya aliran data (bertingkat) dalam akses data.	2	180
DA04			Tidak cocoknya data pada sistem dengan data fisik	Integritas data	4	Kesalahan operator/pegawai yang menginputkan data	4	Validasi dan verifikasi dokumen	1	16
DA05			Data Hilang	Integritas dan ketersediaan data	9	Kegagalan *software*, jaringan	4	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	3	108
DA06			Cybercrime (hacker attack)	Kerahasiaan, integritas ataupun ketersediaan data terancam	10	Kurangnya keamanan pada sistem (*firewall*)	3	Penggunaan VPN sebagai proteksi jaringan	2	60

Code	*Process Function (Category)*	*Critical Assets*	*Potential Failure Modes (process defects)*	*Potential Effect(s) of Failure*	*SEV*	*Potential Cause(s) of Failure*	*OCC*	*Current Process Controls*	*DET*	*RPN*
DA07			Data Korup	Data tidak dapat diakses ataupun data rusak	9	Jaringan internet yang kurang optimal.	7	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	5	315
NT01	Network	Internet, intranet	Koneksi Jaringan putus	Sistem tidak dapat diakses	6	Kegagalan jaringan	9	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	7	378
NT02			Koneksi Jaringan putus	Sistem tidak dapat diakses	6	Rusaknya perangkat jaringan dan atau mati lampu	7	Melakukan pengecekkan terhadap infrastruktur TI yang rusak, menunggu lampu hidup kembali.	6	252
NT03			Konektivitas jaringan menurun	Sistem error, backup failure, data korup.	7	Kegagalan jaringan	10	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	9	630
NT04			Adanya kesalahan pengalamatan IP	Tidak dapat koneksi jaringan	4	*Human error*	2	Melakukan pengecekkan terhadap infrastruktur TI yang rusak	2	16

4.1.3.3.Hasil RPN Tim 1

Berdasarkan penilaian risiko yang telah dilakukan oleh tim 1, dilakukan perhitungan nilai RPN. Perhitungan berdasarkan rumus RPN yaitu dengan mengalikan nilai dari ketiga paramter (*severity*, *occurrence*, detection). Kemudian, pemeringkatan tingkat risiko dilakukan berdasarkan *range* risiko. Berikut ini adalah hasil RPN dari tim 1:

Tabel 4.8. Hasil RPN Tim 1

Code	***Event Risk***	***Potential Cause(s) of Failure***	***RPN***	***Risk Level***
NT03	Konektivitas jaringan menurun	Kegagalan jaringan	600	Very High
HW04	*Server* down	Terlalu banyaknya unit yang mengakses *server* pada waktu bersamaan ataupun serangan DDOS.	378	Very High
NT01	Koneksi Jaringan putus	Kegagalan jaringan	360	Very High
HW05	Kerusakan *server*	Tidak adanya proses *controlling* dan *maintenance* secara rutin	144	High
HW14	Kegagalan jaringan	Kerusakan pada infrastruktur jaringan seperti *switch/hub, router, access point*.	144	High
HW16	Kerusakan Perangkat Jaringan	Bencana alam (*force of nature*) dan atau hewan	126	High
HW13	Akses informasi PC secara ilegal	Penjagaan hak akses lemah dan atau komputer tidak diberi *password.*	100	Medium
DA03	Pembobolan data/informasi	Penyebaran informasi rahasia oleh pegawai (berbagi *password*)	80	Medium
HW15	Kegagalan jaringan	Manipulasi konfigurasi jaringan.	72	Low
HW06	Kerusakan *server*	Bencana alam seperti terkena reruntuhan bangunan (*server* terletak di lantai bawah)	64	Low
HW02	Kebakaran *Server*	Hubungan arus pendek (*power failure*)	60	Low
HW03	*Serveroverheat*	Tidak berfungsinya AC pada ruangan *server*	60	Low
HW08	Komputer tidak dapat digunakan	Kesalahan dalam konfigurasi komputer	60	Low
DA04	Tidak cocoknya data pada sistem dengan data fisik	Kesalahan operator/pegawai yang menginputkan data	60	Low
DA06	Cybercrime (hacker attack)	Kurangnya keamanan pada sistem (*firewall*)	60	Low
HW18	Kerusakan *Printer/ scanner*	*Maintenance* dan kontrol yang tidak rutin.	48	Low
SW01	Kegagalan *Software*	Lisensi *software* yang digunakan sudah melebihi batas waktu	48	Low
PP01	Kegagalan Manusia (*Human*	kesalahan dalam penginputan data dan penggunaan perangkat sistem	48	Low

	failure)			
PP02	Kegagalan Manusia (*Human failure*)	SDM kurang kompeten	48	Low
SW02	Serangan Virus	Antivirus tidak mampu mendeteksi dan mencegah virus yang masuk	36	Low
NT02	Koneksi Jaringan putus	Rusaknya perangkat jaringan dan atau mati lampu	36	Low
HW01	Kebakaran *Server*	*Server* mengalami *overheat*	30	Low
DA05	Data Hilang	Kegagalan *software*, jaringan	30	Low
DA07	Data Korup	Jaringan internet yang kurang optimal.	30	Low
HW07	Kerusakan Komputer	Adanya serangan virus	28	Low
DA01	Penuhnya kapasitas	Kurangnya pengontrolan kapasitas memori *server* dan storage yang telah terpakai	24	Low
DA02	Tersebarnya informasi rahasia	Penyalahgunaan hak akses	18	Very Low
HW09	Komputer tidak dapat digunakan	Lisensi *software* yang digunakan sudah melebihi batas waktu	15	Very Low
HW10	Komputer tidak dapat digunakan	Bencana alam (kebakaran, banjir, petir)	14	Very Low
HW17	Hilangnya komponen perangkat jaringan	Pencurian	12	Very Low
NT04	Adanya kesalahan pengalamatan IP	*Human error*	12	Very Low
PP03	Pemalsuan atau penyalahgunaan hak akses	Adanya kerjasama dengan pihak luar untuk melakukan pemalsuan tanda tangan yang tercatat pada sistem	8	Very Low
SW03	Kegagalan sistem	Sistem masih terdapat celah keamanan	6	Very Low
HW12	Hilangnya komponen PC	Pencurian	3	Very Low
HW20	Hilangnya *printer/ scanner*	Pencurian	2	Very Low
HW11	Perangkat komputer *out of dated*	Usangnya teknologi yang digunakan	1	Very Low
HW19	Kerusakan *Printer/ scanner*	Terjadinya bencana alam seperti banjir, kebakaran, tersambar petir. (*Force of nature*)	1	Very Low

Sumber: Olahan Peneliti, 2018

4.1.3.4.Hasil RPN Tim 2

Berdasarkan penilaian risiko yang telah dilakukan oleh tim 2, dilakukan perhitungan nilai RPN. Perhitungan berdasarkan rumus RPN yaitu dengan mengalikan nilai dari ketiga paramter (*severity*, *occurrence*, detection). Kemudian, pemeringkatan tingkat risiko dilakukan berdasarkan *range* risiko. Berikut ini adalah hasil RPN Tim 2:

Tabel 4.9. Hasil RPN Tim 2

Code	***Event Risk***	***Potential Cause(s) of Failure***	***RPN***	***Risk Level***
NT03	Konektivitas jaringan menurun	Kegagalan jaringan	630	Very High
HW04	*Server* down	Terlalu banyaknya unit yang mengakses *server* pada waktu bersamaan ataupun serangan DDOS.	441	Very High
NT01	Koneksi Jaringan putus	Kegagalan jaringan	378	Very High
DA07	Data Korup	Jaringan internet yang kurang optimal.	315	Very High
HW13	Akses informasi PC secara ilegal	Penjagaan hak akses lemah dan atau komputer tidak diberi *password.*	300	Very High
HW16	Kerusakan Perangkat Jaringan	Bencana alam (*force of nature*) dan atau hewan	294	Very High
NT02	Koneksi Jaringan putus	Rusaknya perangkat jaringan dan atau mati lampu	252	Very High
HW05	Kerusakan *server*	Tidak adanya proses *controlling* dan *maintenance* secara rutin	196	High
DA03	Pembobolan data/informasi	Penyebaran informasi rahasia oleh pegawai (berbagi *password*)	180	High
DA05	Data Hilang	Kegagalan *software*, jaringan	108	Medium
HW14	Kegagalan jaringan	Kerusakan pada infrastruktur jaringan seperti *switch/hub, router, access point.*	72	Low
DA02	Tersebarnya informasi rahasia	Penyalahgunaan hak akses	60	Low
DA06	Cybercrime (hacker attack)	Kurangnya keamanan pada sistem (*firewall*)	60	Low
DA01	Penuhnya kapasitas	Kurangnya pengontrolan kapasitas memori *server* dan storage yang telah terpakai	50	Low
PP02	Kegagalan Manusia (*Human failure*)	SDM kurang kompeten	48	Low
PP01	Kegagalan Manusia (*Human failure*)	kesalahan dalam penginputan data dan penggunaan perangkat sistem	45	Low
SW01	Kegagalan *Software*	Lisensi *software* yang digunakan sudah melebihi batas waktu	40	Low

HW18	Kerusakan *Printer/ scanner*	*Maintenance* dan kontrol yang tidak rutin.	36	Low
HW19	Kerusakan *Printer/ scanner*	Terjadinya bencana alam seperti banjir, kebakaran, tersambar petir. (*Force of nature*)	36	Low
PP03	Pemalsuan atau penyalahgunaan hak akses	Adanya kerjasama dengan pihak luar untuk melakukan pemalsuan tanda tangan yang tercatat pada sistem	36	Low
HW07	Kerusakan Komputer	Adanya serangan virus	28	Low
SW02	Serangan Virus	Antivirus tidak mampu mendeteksi dan mencegah virus yang masuk	25	Low
DA04	Tidak cocoknya data pada sistem dengan data fisik	Kesalahan operator/pegawai yang menginputkan data	16	Very Low
NT04	Adanya kesalahan pengalamatan IP	*Human error*	16	Very Low
HW03	*Serveroverheat*	Tidak berfungsinya AC pada ruangan *server*	12	Very Low
HW08	Komputer tidak dapat digunakan	Kesalahan dalam konfigurasi komputer	12	Very Low
HW15	Kegagalan jaringan	Manipulasi konfigurasi jaringan.	12	Very Low
HW17	Hilangnya komponen perangkat jaringan	Pencurian	12	Very Low
HW09	Komputer tidak dapat digunakan	Lisensi *software* yang digunakan sudah melebihi batas waktu	9	Very Low
SW03	Kegagalan sistem	Sistem masih terdapat celah keamanan	5	Very Low
HW01	Kebakaran *Server*	*Server* mengalami *overheat*	4	Very Low
HW02	Kebakaran *Server*	Hubungan arus pendek (*power failure*)	1	Very Low
HW06	Kerusakan *server*	Bencana alam seperti terkena reruntuhan bangunan (*server* terletak di lantai bawah)	1	Very Low
HW10	Komputer tidak dapat digunakan	Bencana alam (kebakaran, banjir, petir)	1	Very Low
HW11	Perangkat komputer *out of dated*	Usangnya teknologi yang digunakan	1	Very Low
HW12	Hilangnya komponen PC	Pencurian	1	Very Low
HW20	Hilangnya *printer/ scanner*	Pencurian	1	Very Low

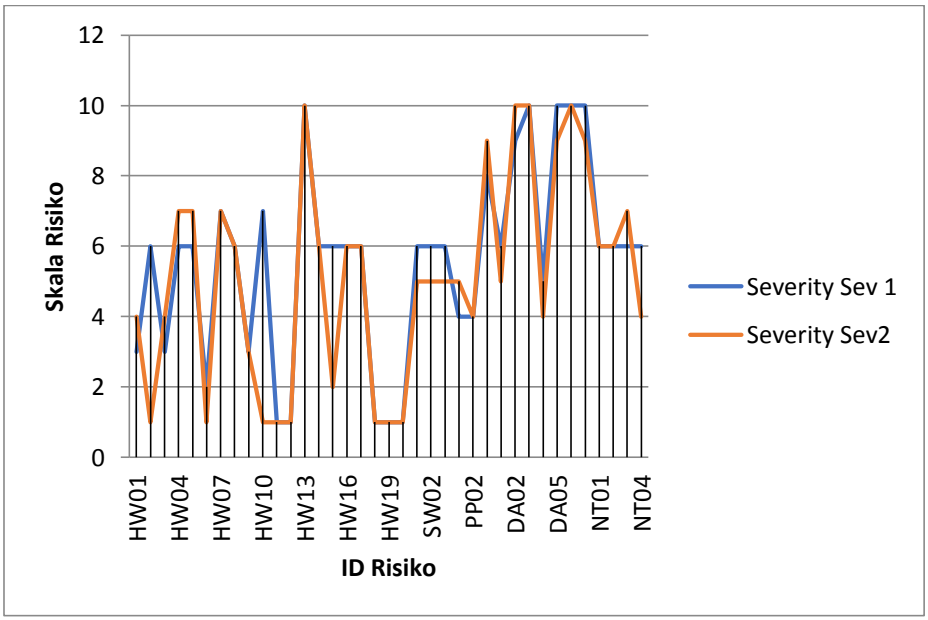
Sumber: Olahan Peneliti, 2018

4.1.4. Analisis Kesenjangan (Gap Analysis)

Analisis kesenjangan didefinisikan dengan penentuan perbedaan pengetahuan atau praktik terkini (yang sedang dilakukan) dengan bukti dari *best practice* (apa yang harus dilakukan) (Janneti, 2012). Tujuan dari analisis kesenjangan untuk melihat perbedaan dari hasil penilaian risiko dari dua tim yang berbeda pada studi kasus yang sama. Perbandingan berdasarkan parameter perbedaan atau faktor-faktor yang telah dikemukakan pada penelitian (Estorilio & Posso, 2010). Terdapat beberapa faktor yang mempengaruhi irregularitas dari pengukuran risiko pada FMEA yaitu dari segi pengetahuan, tim yang mengukur risiko, pelatihan, *failure history*, dan waktu penyelesaian. Faktor tersebut menjadi kategorisasi untuk melihat perbedaan dari kedua tim FMEA dan ditambah dengan perbedaan jawaban dari kedua tim. Untuk memperjelas perbedaan, berikut ini dijabarkan terlebih dahulu perbedaan yang terdapat dari jawaban yang diperoleh dari kedua tim pada ketiga parameter FMEA (*severity, occurrence* dan *detection*):

1. Perbedaan Jawaban Tingkat Keparahan

Jawaban dari tim 1 dan tim 2 dalam menjawab tingkat keparahan masing masing risiko banyak perbedaan. Perbedaan tersebut dapat terlihat pada gambar di bawah ini:

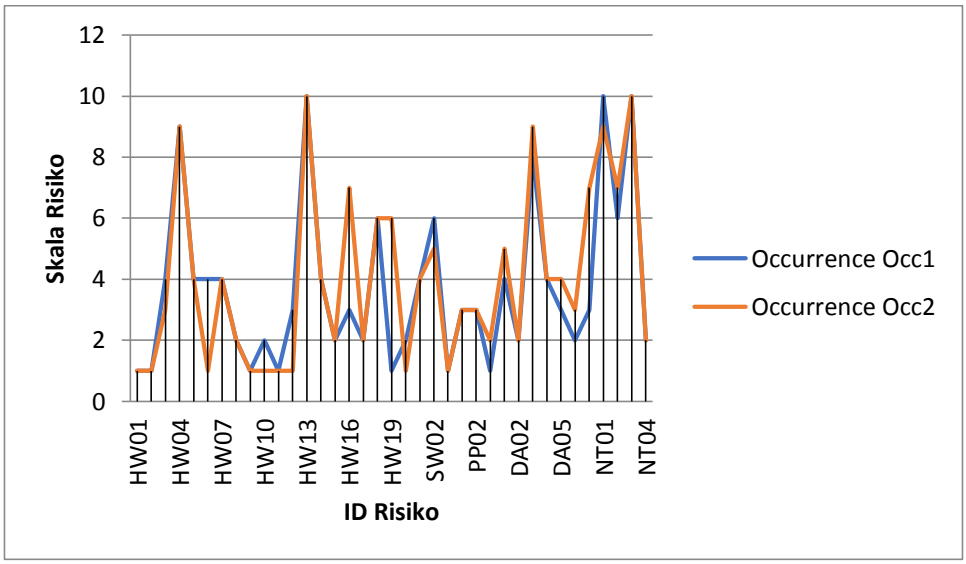


Gambar 4.1. Perbandingan Jawaban *Severity* (Tim 1)

Perbedaan persepsi dalam tingkat keparahan pada satu risiko yang sama. Terdapat perbedaan yang jauh seperti ID Risiko HW02, tim 1 menjawab tingkat keparahan 6, sedangkan tim 2 menjawab tingkat keparahan 1. Demikian juga dengan ID Risiko HW10, tim 1 menjawab tingkat keparahan 7, sedangkan tim 2 menjawab tingkat keparahan 1. Perbedaan dalam pemberian nilai ini tentunya berpengaruh signifikan dengan hasil perangkingan risiko. Dikarenakan kedudukan tiap parameter adalah sama (linier), sehingga jika dikalikan dengan nilai lainnya akan sangat mempengaruhi besaran nilai RPN yang diperoleh.

2. Perbedaan Jawaban Tingkat Terjadi (Occurrence)

Jawaban dari tim 1 dan tim 2 dalam menjawab tingkat terjadi masing masing risiko tidak terlalu banyak perbedaan. Perbedaan tersebut dapat terlihat pada gambar di bawah ini:

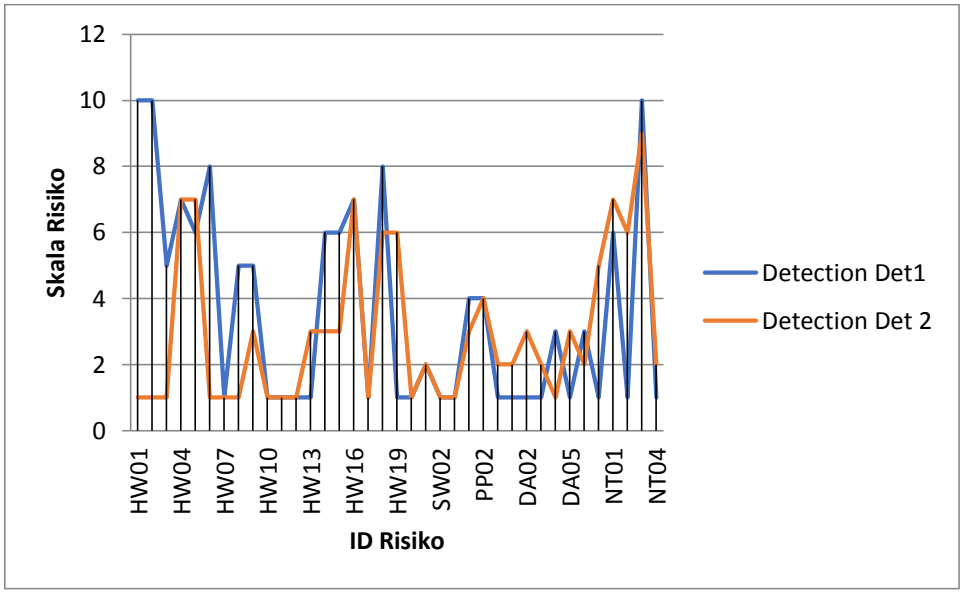


Gambar 4.2. Perbandingan Jawaban *Occurrence* (Tim 1)

Berdasarkan grafik diatas, perbedaan jawaban antar satu risiko dengan risiko lainnya tidak terlalu jauh. Hal ini membuktikan kedua tim memahami kejadian risiko yang terjadi dengan lingkungan yang sedang mereka jalani. Bahwasanya, risiko yang ada bisa diprediksi berdasarkan tingkat terjadinya dengan mendefinisikannya dengan skala rentang waktu.

3. Perbedaan Jawaban Tingkat Deteksi (Detection)

Jawaban dari tim 1 dan tim 2 dalam menjawab tingkat terjadi masing masing risiko banyak terjadi perbedaan. Perbedaan tersebut dapat terlihat pada gambar di bawah ini:



Gambar 4.3. Perbandingan Jawaban *Detection* (Tim 1)

Berdasarkan grafik diatas, perbedaan jawaban dalam memberikan nilai *detection* banyak terjadi perbedaan. Seperti salah satu contoh adalah risiko dengan ID Risiko HW01 dan HW 02, tim 1 menjawab bahwa tingkat deteksi risiko bernilai 10, sedangkan tim 2 menjawab bahwa tingkat deteksi risiko bernilai 1.

Dari jawaban kedua tim, perbedaan jawaban yang paling signifikan secara berurutan terjadi pada parameter tingkat deteksi, kemudian pada tingkat keparahan dan terakhir pada tingkat terjadi. Ketiga parameter tersebut dikalkulasi sesuai dengan rumus RPN (*severity x occurrence x detection*) kemudian dilakukan pengurutan nilai RPN yang paling tinggi hingga nilai RPN yang paling rendah. Perolehan RPN pada tim pertama adalah 3 risiko berada pada level *very high*, sedangkan pada tim kedua adalah 6 risiko berada pada level *very high*.

Perbedaan selanjutnya dilihat dari aspek orang. Orang yang dimaksudkan adalah tim 1 dan tim 2 yang melakukan pengukuran risiko. Tim 1 beranggotakan satu orang Kepala Seksi SISKOHAT, satu orang praktisi TI, dan satu orang

sebagai koordinator tim. Sedangkan tim 2 beranggotakan satu orang operator, satu orang praktisi TI, dan satu orang sebagai koordinator tim.

Praktisi TI pada tim pertama adalah Dr. Okfalisa, S.T., M.Sc. Beliau merupakan Dosen dan sekaligus menjabat sebagai Wakil Dekan III pada Fakultas Sains dan Teknologi UIN SUSKA Riau. Pemilihan praktisi melihat kualifikasi yang dimiliki oleh beliau dalam bidang Teknologi dan Sistem Informasi. Praktisi TI pada tim kedua adalah Eki Saputra, S.Kom., M.Kom. Beliau adalah Dosen pada jurusan sistem informasi, Fakultas Sains dan Teknologi, UIN SUSKA Riau. Pemilihan praktisi telah sesuai dengan kualifikasi yang telah ditentukan. Beliau juga merupakan dosen pengampu mata kuliah Keamanan Sistem Informasi serta Jaringan Komputer dan Bisnis. Sehingga, kualifikasi Beliau sesuai dengan yang dibutuhkan dalam penelitian ini.

Profil informan yang menjadi narasumber dalam penilaian risiko adalah Bapak Drs. H. Asril selaku Kepala Seksi SISKOHAT. Beliau telah menjabat sebagai KASI SISKOHAT selama 2 tahun dan sebelumnya menjabat sebagai KASI Pembinaan Haji dan Umrah lebih kurang 5 tahun. Kemudian, pada tim kedua adalah Bapak Nik Yusri selaku operator SISKOHAT yang telah bekerja sebagai operator selama 15 tahun.

Dari segi waktu penyelesaian, tim 1 lebih sedikit lama dibandingkan tim kedua. Tim pertama memulai penilaian risiko dari pukul 09.00 WIB hingga 12.00 WIB. Sedangkan tim kedua, mulai dari pukul 14.00 WIB hingga 15.30 WIB. Tim pertama cenderung lebih banyak memakan waktu dalam memberikan pemahaman akan risiko yang akan berdampak dari segi keparahan, deteksi dan tingkat terjadinya. Sehingga, tim pertama lebih cenderung pasif dalam memberikan penilaian risiko. Sedangkan tim kedua, penilaian risiko berlangsung lebih atraktif karena informan memberikan informasi yang lebih detail sehingga dalam penilaian risiko lebih cepat terselesaikan.

Jumlah pelatihan teknis SISKOHAT, setiap tahunnya operator dan KASI SISKOHAT mengikuti pelatihan yang diadakan oleh Kementerian Agama Pusat. Akan tetapi, pengalaman pada operator dalam menggunakan SISKOHAT lebih lama dibandingkan KASI SISKOHAT. Operator menggunakan SISKOHAT selama 15 tahun, sedangkan KASI SISKOHAT kurang dari 10 tahun. Hal ini

dikarenakan adanya mutasi pejabat yang dilakukan, sehingga KASI SISKOHAT mengetahui secara umum dan menjalankan fungsi *monitoring* terhadap SISKOHAT melalui operator.

Dari segi pengetahuan, kedua informan belum pernah menggunakan metode FMEA. Pada Bidang Penyelenggaraan haji dan umrah juga belum pernah dilakukan pengukuran risiko Teknologi Informasi sehingga dari faktor *failure histroy* hanya bergantung pada pengalaman pengetahuan dari informan. Hal ini juga dipengaruhi oleh latar belakang pendidikan informan bukan berasal dari Teknologi Informasi, sehingga perlu memberikan pemahaman terlebih dahulu terkait daftar risiko yang didefinisikan.

Dari pemaparan kesenjangan diatas, dapat dirangkum dalam tabel berikut ini:

Tabel 4.10. Kesenjangan tim 1 dan tim 2

No	Faktor	Perbedaan *(Current Practice)*	*What is the Best Practice?*
1	Perbandingan jawaban ketiga parameter (*severity, occurrence, detection*)	RPN pada tim 1 terdapat 3 risiko yang berada pada level *very high* sedangkan tim 2 terdapat 6 risiko yang berada pada level *very high*. Dari perbedaan jawaban, urutan yang paling membedakan secara signifikan adalah jawaban pada kontrol (deteksi) risiko, tingkat keparahan, dan tingkat terjadi.	Membatasi ukuran variabel parameter (Skala) dapat menjadikan FMEA menjadi metode yang lebih cepat, menjadi lebih efektif serta menghasilkan hasil yang kuat. (Paciarotti et al., 2014)
2	Orang(Tim FMEA)	Tim pertama terdiri praktisi TI, KASI SISKOHAT, dan fasilitator (koordinator). Sedangkan tim kedua terdiri dari Praktisi TI, Operator dan fasilitator (koordinator).	Sudah sesuai dengan hasil penelitian Odenholf, et al (2011) yaitu paling sedikit ada dua teknisi ahli yang termasuk dalam tim FMEA untuk menyeimbangkan perbedaan individu yang signifikan dalam keputusan risiko yang krusial. Jumlah

			tim yang ganjil membantu dan memudahkan dalam proses perhitungan *voting*.
3	Waktu Penyelesaian	Tim pertama memakan waktu yang lebih lama dibandingkan tim kedua. Tim kedua lebih atraktif dalam menilai risiko.	Pondasi dari FMEA adalah anggota tim dan hasil masukan dari proses FMEA dan perlu adanya estimasi waktu dan pembagian tugas yang jelas (McDermott et al., 2009). Tidak lebih dari 90 menit(Estorilio & Posso, 2010).
4	Training	Kedua tim dilakukan penjelasan dalam menggunakan metode FMEA. Informan telah mendapatkan pelatihan terkait SISKOHAT setiap tahunnya yang diadakan oleh Pusat. Operator lebih menguasai SISKOHAT dikarenakan pengalamannya menggunakan sistem tersebut selama 15 tahun. Sedangkan, KASI SISKOHAT selalu adanya pergantian (mutasi pejabat) sehingga pemahaman alur SISKOHAT penggunaannya sebagai fungsi *monitoring*.	Adanya pelatihan terkait metode FMEA dan perkenalan terhadap risiko TI(Estorilio & Posso, 2010).
5	Pengetahuan (*Knowledge*)	Pada Bidang Penyelenggaraan haji dan umrah juga belum pernah dilakukan pengukuran risiko Teknologi Informasi sehingga. Hal ini juga dipengaruhi oleh latar belakang pendidikan informan bukan berasal dari Teknologi	

		Informasi.	
6	*Failure History*	Faktor *failure histroy* hanya bergantung pada pengalaman pengetahuan dari informan. Informan kedua (operator) telah bekerja sebagai operator selama 15 tahun, sedangkan KASI SISKOHAT selama 2 tahun dan sebelumnya lebih kurang 5 tahun menjabat sebagai KASI Pembinaan Haji dan Umrah pada Bidang Penyelenggaraan Haji dan Umrah.	

Sumber: Olahan Peneliti, 2018

Pembahasan selanjutnya dan solusi perbaikan secara rinci dilakukan pada siklus *action research* kedua dan menguji coba konsistensi FMEA yang disintesis pada studi kasus. Solusi perbaikan berdasarkan kesenjangan hasil dari kedua tim menjadi bagian pertimbangan dalam melakukan modifikasi perbaikan kerangka FMEA. Sintesis kerangka FMEA dibahas pada subbab sintesis kerangka FMEA yang menjadi *closing the gap.*

4.2. Siklus 2. *Action research* Sintesis FMEA (*Improvement*)

Berikut ini penjabaran hasil dari siklus pertama dalam *action research* sintesis FMEA. Implementasi FMEA yang telah disintesis dilakukan dengan mengikuti kerangka yang telah diformulasikan.

4.2.1. Skenario *Action research* 2

Skenario yang dideskripsikan pada tabel 4.11. adalah panduan dalam melakukan *action research* untuk siklus kedua. Skenario dilakukan sebagai kontrol peneliti dalam melakukan penelitian. Tahapan proses dimulai dengan melakukan sintesis kerangka FMEA sebagai perbaikan atau *improvement* dari hasil siklus *action research* pertama. Langkah sintesis FMEA adalah dengan menganalisa kelemahan tahapan FMEA, kemudian memberikan rekomendasi

solusi perbaikan dengan mempertimbangkan hasil dari *action research* pertama dan studi literatur. Setelah itu, dilakukan validasi oleh pakar agar kerangka FMEA yang telah disintesis dapat digunakan dan diuji coba pada studi kasus. Pengimplementasian FMEA dilakukan kembali pada Kantor Wilayah Kementerian Agama Provinsi Riau, Bidang Penyelenggaraan Haji dan Umrah. Tim FMEA yang digunakan adalah tetap seperti pada siklus pertama. Hal ini untuk melihat perbedaan hasil RPN yang diperoleh *action research* kedua dari kedua tim yang sama dengan studi kasus yang sama seperti siklus *action research* implementasi FMEA Tradisional.

Pada siklus pertama menghasilkan hasil analisis kesenjangan hasil pengukuran risiko oleh kedua tim. Kesenjangan dilihat berdasarkan perbedaan peringkat (ranking) dari RPN. Siklus kedua menjadi solusi perbaikan dalam mengatasi isu konsistensi yang ditemukan pada siklus pertama. Penilaian konsistensi siklus kedua ini juga akan dilihat dari kesenjangan hasil RPN dari kedua tim. Sehingga, dengan adanya perbandingan kesenjangan RPN dari kedua tim dan dari kedua siklus akan diketahui keberhasilan dalam perbaikan konsistensi FMEA.

Tabel 4.11. Skenario Siklus *Action research* 2

Tahapan	Indeks Proses	Proses	Indeks Skenario	Skenario	Luaran yang Diharapkan	Data Skenario
Sinstesis Kerangka FMEA	P1	Kritikal analisis kerangka FMEA	P1.1	Melakukan studi literatur terhadap kelemahan pada kerangka FMEA dan diperkuat dengan hasil *action research* pertama	Titik kelemahan FMEA pada tahapannya berdasarkan dokumen FMEA.	- Hasil *action research* pertama - Studi Literatur - Hasil Validasi Pakar
		Mendiagnosis penyebab kelemahan kerangka FMEA	P1.2	Mencari faktor penyebab FMEA menjadi tidak konsisten.	Mengetahui faktor penyebab FMEA tidak konsisten.	
		Usulan perbaikan	P1.3	Memberikan solusi perbaikan berdasarkan literatur yang ditemukan.	Alur metodologi FMEA yang disintesis (*FMEA Improvement*).	
Validasi Pakar	P2	Validasi kerangka FMEA yang diperbaiki oleh pakar	P2.1	Melakukan konsultasi kepada pakar terkait kerangka FMEA yang telah disintesis.	Kerangka FMEA yang disintesis tervalidasi.	
Implementasi Kerangka FMEA yang disintesis (FMEA *Improvement*)	P3	Identifikasi Konteks	P3.1	Perumusan tujuan, ruan lingkup pengukuran risiko, objek pengukuran risiko, indikator kinerja, komponen aset	Sebagai bahan pembuatan prosedur dalam pembuatan tim FMEA pada fase selanjutnya.	- Hasil siklus *action research* pertama
		Identifikasi Proses Bisnis	P3.2	Menganalisa proses bisnis yang ada pada studi kasus.	Analisa proses bisnis	- Hasil siklus *action research*

						pertama
		Pembentukan tim FMEA (KABID Penyelenggaraan Haji dan umrah, KASI SISKOHAT, Peneliti)	P3.3	Membentuk tim yang sesuai dengan kriteria yang ditentukan dan melakukan pengesahan (prosedur pembentukan tim)	Tim FMEA	- Dokumen prosedur tim FMEA
		Menentukan metode penilaian	P3.4	Menentukan metode penelitian (desain dokumen FMEA dan skala kriteria)	Dokumen FMEA *improvement* dan skala kriteria pengukuran	- Hasil validasi pakar
		Pelatihan dan pemahaman prosedur	P3.5	Pemberian panduan dan penjelasan materi FMEA *improvement* kepada tim FMEA.	Modul panduan pengukuran risiko dengan FMEA *improvement*	- Kerangka FMEA *improvement* yang sudah divalidasi
		Brainstorming potensi kegagalan	P3.6	Merumuskan potensi kegagalan dengan mendefinisikan aset kritis, membangun profil berbasis ancaman, profil aset berbasis ancaman, identifikasi kelemahan infrastruktur.	Bahan untuk mengisi pentabelan FMEA *improvement.*	- Hasil siklus *action research* pertama
		Penyusunan *risk register* / daftar	P3.7	Menyusun daftar risiko dalam tabel FMEA *improvement*.	Dokumen FMEA *improvement*	- Hasil *brainstorming*

		risiko				potensi kegagalan
		Pemberian nilai tingkat pada masing-masing parameter. (tim FMEA)	P3.8	Penilaian risiko oleh dua tim dan limitasi waktu pengukuran <90 menit.	Hasil pengukuran risiko	- Dokumentasi
		Perhitungan RPN	P3.9	Mengkalkulasikan nilai risiko yang didapat.	Nilai RPN	- Dokumentasi
		Pemrioritasan Risiko	P3.10	Melakukan pengurutan risiko	Pemeringkatan risiko	Dokumentasi
		Rekomendasi kontrol	P3.11	Penjelasan rekomendasi kontrol	-	-
Penarikan Kesimpulan	P4	Perbandingan dan Pembahasan kedua siklus *action research*	P4.1	Melakukan pembahasan siklus *action research*kedua dan membahas keseluruhan dari impelementasi kedua siklus *action research.*	Kesimpulan penelitian dan penelitian selanjutnya untuk pengembangan penelitian ini.	- Hasil pembahasan siklus *action research*pertama -Hasil pembahasan siklus *action research* kedua

Sumber: Olahan Peneliti, 2018

4.3. Sintesis Kerangka FMEA (*FMEA Improvement*)

Sintesis kerangka FMEA terdiri dari tiga tahapan yaitu kritikal analisis, diagnosis penyebab, dan sintesis kerangka FMEA sebagai usulan rekomendasi. Kritikal analisis merupakan hasil ulasan dari literatur terkait kelemahan atau limitasi dari FMEA, kemudian setelah itu dilakukan diagnosa penyebab. Diagnosa bertujuan untuk mengidentifikasi faktor terjadinya konsistensi FMEA berdasarkan literatur dan hasil dari *action research* pertama. Perbaikan usulan rekomendasi dilakukan untuk dapat mendapatkan metodologi FMEA yang telah ditingkatkan berdasarkaan hasil dari ulasan literatur dan *action research* pertama.

4.3.1. Kritikal Analisis

Kritikal analisis ini bertujuan untuk mendefinisikan kelemahan kerangka FMEA tradisional. Kelemahan-kelemahan tersebut didasarkan pada literatur yang ditemukan. Literatur-literatur yang membahas kelemahan tersebut diulas, sehingga didapatkan titik kelemahan dari tahapan FMEA tradisional. Penggunaan FMEA secara luas dan umum dilakukan dalam manajemen risiko. Risiko yang dimaksudkan pada penelitian ini adalah risiko Teknologi Informasi (TI).

Risiko TI juga berkaitan dengan ancaman dan bahaya karena pemakaian TI secara intensif yang mungin menyebabkan kerusakan yang tidak diinginkan atau tidak terduga, kesalahan penggunaan dan kerugian dalam keseluruhan model bisnis dan termasuk lingkungannya(Spremic & D, 2008). Risiko adalah sesuatu yang tidak diinginkan terjadi, maka risiko TI tersebut perlu dilakukan pengelolaan oleh organisasi. Menurut Gottfried (1989), tujuan dari manajemen risiko TI adalah untuk melindungi aset TI seperti data, perangkat keras, perangkat lunak, personal dan fasilitas dari seluruh ancaman faktor eksternal (seperti: bencana alam) dan faktor internal (seperti: kesalahan teknis, sabotase, akses yang tidak terotorisasi) (Bandyopadhyay et al., 2011). Kemudian, menurut Rainer et al (1991), tujuan lain manajemen risiko adalah untuk menghindari atau mengurangi kerugian dengan memilih dan menerapkan kombinasi terbaik dari tindakan (Bandyopadhyay et al., 2011). Dengan adanya manajemen risiko dapat meminimalisir biaya yang akan dikeluarkan jika ternyata kejadian risiko tersebut benar terjadi.

Metode dalam manajemen risiko adalah kualitatif, kuantitatif dan semi kuantitatif. Metode yang murni kualitatif dan deskriptif cenderung lebih subjektif

hasil penilaian risikonya. Sedangkan, metode yang kuantitatif saja dapat menghilangkan banyak informasi, menghabiskan banyak waktu dan sulitnya mendeskripsikan risiko yang ada pada suatu organisasi(Chen, 2015). Menurut (Lai & Chin, 2014), sebagian besar dari metode ataupun *tools* dari manajemen risiko adalah kualitatif dan deskriptif. Sedangkan, FMEA diklasifikasikan dalam semi kuantitatif. Sehingga selama proses FMEA, angka RPN dari potensial kegagalan dapat mendukung analisis kuantitatif dari kejadian risiko, dan metode ini bukan hanya menemukan tingkat tinggi risiko secara tepat dan cepat, tetapi juga mengatasi kekhawatiran kehilangan dan meningkatkan reliabilitas sebuah produk ataupun jasa (Zhao & Bai, 2010). Tidak seperti prosedur pengukuran risiko lainnya, FMEA dapat mengevaluasi secara kritis dari risiko yang potensial (Murphy et al., 2011).

Disamping kemudahan dan keunggulan dari FMEA tersebut, FMEA memiliki limitasi atau kekurangan berdasarkan literatur yang telah diulas. Berdasarkan hasil *literature review* yang dilakukan oleh (Liu et al., 2013) terdapat beberapa kekurangan dari FMEA tradisional yang telah dikritisi oleh banyak peneliti, diantaranya adalah:

1. Tingkat kepentingan relatif dari faktor risiko yang tidak dipertimbangkan pada pendekatan tradisional.
2. Adanya perbedaan kombinasi dari faktor risiko yang mungkin akan menghasilkan nilai RPN yang sama tetapi sesungguhnya memiliki nilai esensi yang mungkin berbeda dan tersembunyi.
3. Ketiga faktor risiko sulit di evaluasi secara tepat.
4. Formulasi matematika dari RPN masih menjadi pertanyaan dan sangat sensitif bagi faktor risiko.
5. Konversi skor berbeda untuk ketiga faktor risiko.
6. RPN tidak dapat digunakan untuk mengukur secara efektif dan aksi korektif.
7. RPN tidak berkelanjutan dengan banyaknya kelemahan.
8. Interdependensi di antara berbagai mode kegagalan dan efeknya tidak diperhitungkan.
9. Bentuk matematika yang diadopsi untuk menghitung RPN sangat sensitif untuk berbagai jenis dari evaluasi faktor risiko.

10. Banyaknya nilai RPN yang duplikat.
11. Tidak mudah bagi *expert* untuk memberikan nilai *input* secara tepat untuk faktor risiko karena sifatnya yang rentan.

Menurut Ericson (2005), dalam menggunakan metode FMEA menggunakan dokumen FMEA (*worksheet*) untuk menyediakan struktur analisis, konsistensi, dan dokumentasi(Raspotnig & Opdahl, 2013). Identifikasi kelemahan dilakukan berdasarkan dokumen FMEA yang dapat dianalisis titik kelemahannya (Estorilio & Posso, 2010). Berikut ini dilakukan identifikasi kelemahan FMEA berdasarkan penelitian terdahulu, yaitu:

1. Daftar Risiko (potensi kegagalan, penyebab, kontrol)

Mode kegagalan sebagai pengamatan dampak dari sebuah kegagalan atau risiko. Kegagalan tersebut akan berdampak pada organisasi. Seharusnya, tidak perlu adanya kebingungan dalam menentukan atau mencari akar masalah dari penyebab dampak yang jarang terlihat dalam sebuah komponen sistem. Bias fokus pada nilai RPN rendah, tetapi risiko nilai konsekuensi keparahan besar harus dapat dicegah. Hal ini juga berlaku untuk risiko yang tingkat terjadinya sering dengan tingkat keparahan kecil karena jika risiko tingkat keparahan yang kecil itu dikalkulasikan dengan frekuensi kejadian yang tinggi akan menjadi risiko yang signifikan besar(Cameron et al., 2017).

Kelemahan dari daftar risiko adalah ketiga faktor risiko sulit dievaluasi secara tepat (Liu et al., 2013). Kesulitan dalam mengevaluasi risiko secara tepat juga dipengaruhi oleh daftar risiko yang terdiri dari banyak risiko dengan skenario risiko yang berbeda. Banyaknya variasi skenario risiko yang berbeda dan direpresentasikan oleh nilai parameter risiko yang menghasilkan nilai RPN yang identik. FMEA tidak memperbolehkan untuk membedakan antara implikasi risiko yang berbeda (Sawhney et al., 2010). Sistem pentabelan yang dimaksudkan FMEA adalah satu risiko, satu penyebab, dan satu kontrol. Hal ini menimbulkan banyaknya daftar risiko.

2. Penilaian dan Skala Kriteria (*severity, occurrence, detection*)

Dalam menggunakan FMEA tradisional faktor risiko/parameter *severity*, *occurrence* dan *detection* didapatkan dari *expert* dalam tim FMEA berdasarkan

skala 5,7, ataupun 10 yang mirip dengan skala *Likert's* (Liu et al., 2013). Dalam penentuan skala ini tidak ada prosedur khusus, sehingga dapat ditentukan sesuai keinginan dari pengukur risiko. Tetapi paling umum digunakan adalah skala 1 hingga 10. Skala kriteria lainnya seperti 1-3 atau 1-5 bisa digunakan, skala kriteria yang berbeda untuk ketiga parameter juga dapat digunakan, ataupun begitu pula untuk skala yang dibuat sendiri oleh anggota tim melalui konsensus tim (van Leeuwen et al., 2009)**.**

Kriteria skala ini menjadi permasalahan jika pendefinisian yang tidak jelas dan batasan yang meragukan. Penelitian (Paciarotti et al., 2014) melakukan modifikasi atau perbaikan dari segi skala FMEA. Hal ini dilakukan untuk meminimalisir kekurangan dari FMEA. Skala 1-10 membuat tim berfikir lebih lama dalam menentukan skala yang tepat karena banyaknya pertimbangan angka yang tepat. Penelitian tersebut mendefinisikan skala (1,3,9) dalam pemberian nilai S, O, D dengan tingkat (*high, medium, low*). Membatasi ukuran variabel parameter dapat menjadikan FMEA menjadi metode yang lebih cepat, menjadi lebih efektif serta menghasilkan hasil yang kuat.

Tidak mudah bagi *expert* untuk memberikan nilai *input* secara tepat untuk faktor risiko karena sifatnya yang rentan (Liu et al., 2013). Skala kriteria ini sangat mempengaruhi pada hasil yang didapatkan pada RPN daftar risiko. Nilai dari skala kriteria berguna untuk membantu dalam mengidentifikasi risiko yang paling serius untuk dilakukan aksi perbaikan. Pada kenyataannya, ketiga parameter tidak berbobot sama terhadap satu sama lain dalam hal risiko. Distorsi ini diperparah oleh sifat non-linear dari skala peringkat individu (1-10)(Sankar & Prabhu, 2001).

3. Tim FMEA

Terdapat isu subjektif karena adanya *human error*dan *bias* dalam melakukan prioritisasi risiko, hal ini merupakan salah satu limitasi yang didapatkan berdasarkan literatur *review* yang telah dilakukan. Kegiatan prioritisasi dilakukan berdasarkan emosi manusia dan pikiran, sehingga terdapat keraguan dalam keakuratan konsep yang tentunya juga berasal dari parameter yang digunakan. Tim FMEA akan sulit menentukan perbedaan opini yang terjadi

dalam perhitungan, dan variabel yang dibutuhkan dalam menghitung angka risiko yang tidak sesuai dan meragukan (Kakvan et al., 2014). Kelemahan lainnya adalah dari segi tim FMEA adanya perbedaan pendapat dalam menentukan nilai dari setiap parameter FMEA. Hal ini menyebabkan RPN yang sama ataupun identik dengan yang lainnya tanpa adanya kemampuan dalam mengartikulasikan implikasi risiko(Sawhney et al., 2010).

FMEA yang memakan waktu dalam proses dan membutuhkan tim yang multidisiplin sehingga memahami dengan baik proses yang dianalisa(Jain, 2017). Walaupun belum adanya panduan ataupun prosedur yang jelas mengenai anggota tim yang seharusnya, hal ini menunjukkan bahwa FMEA merupakan metode yang sedikit lebih eksplisit dibandingkan metode lainnya(Raspotnig & Opdahl, 2013).

4. RPN (*Risk Priority Number*)

Teknik RPN menggunakan istilah linguistik untuk menentukan tingkat keparahan dari dampak risiko (kegagalan), kemungkinan terjadinya risiko dan peluang risiko dapat dideteksi menggunakan skala 1 hingga 10. Nilai dari ketiga parameter tersebut dikalikan sehingga diperoleh RPN. Risiko yang memiliki nilai RPN tertinggi diasumsikan sebagai risiko yang penting dan mendapatkan prioritas penanganan yang tinggi dibandingkan risiko yang memiliki nilai RPN yang rendah (Ford Motor Company, 1988) dalam (Sankar & Prabhu, 2001). Secara tradisional, keputusan untuk meningkatkan sebuah proses operasional adalah berdasarkan pada prioritas dari hasil RPN FMEA. Metode ini sangat *powerful* dan berguna dalam melakukan penilaian risiko. RPN digunakan dalam pengukuran risiko dengan berdasarkan parameter (Xiao et al., 2011):

a. *Severity* (S): Hasil yang dihasilkan dari *failure* (risiko)
b. *Occurrence* (O): Peluang ataupun kesempatan terjadinya *failure* (risiko)
c. *Detection* (D) : Peluang untuk risiko yang tidak teridentifikasi karena susahnya dalam mendeteksi.

Berdasarkan (Chai, Jong, Tay, & Lim, 2016), skor RPN memiliki kelemahan yaitu:

a. Skor RPN tidak mempertimbangkan kepentingan relatif yang berkaitan dengan S, O, dan D.
b. Sementara skor RPN yang sama dapat dihasilkan oleh kombinasi dari S, O, dan D yang berbeda, implikasi risiko yang mendasarinya dapat berbeda.
c. Tidak mudah untuk secara tepat menilai S, O, dan D.
d. Metode untuk menghitung skor RPN (yaitu, dengan mengalikan S, O, dan D) terbuka untuk diskusi, karena tidak kuat dalam hal mengevaluasi faktor-faktor kritis.

Menurut hasil ulasan literatur penelitian terdahulu terkait kelemahan RPN secara spesifik adalah (Liu et al., 2013):

a. Tingkat kepentingan relatif dari faktor risiko yang tidak dipertimbangkan pada pendekatan tradisional.
b. Formulasi matematika dari RPN masih menjadi pertanyaan dan sangat sensitif bagi faktor risiko.
c. Konversi skor berbeda untuk ketiga faktor risiko
d. RPN tidak dapat digunakan untuk mengukur secara efektif dan aksi korektif.
e. RPN tidak berkelanjutan dengan banyaknya kelemahan.
f. Bentuk matematika yang diadopsi untuk menghitung RPN sangat sensitif untuk berbagai jenis dari evaluasi faktor risiko.
g. Banyaknya nilai RPN yang duplikat.

Permasalahan RPN dikarenakan ketiga parameter dalam nilai yang sama penting. Menurut hasil ulasan literatur yang dilakukan oleh (Liu et al., 2013) bahwa kelemahan FMEA adalah tingkat kepentingan relatif dari faktor risiko yang tidak dipertimbangkan pada pendekatan tradisional. RPN konvensional FMEA tidak memiliki bobot nilai karena memiliki tingkat penting yang sama pada setiap parameter (*severity*, *occurrence,* dan *detection*). Dan banyaknya variasi kombinasi dapat menyebabkan samanya nilai RPN. Dengan demikian layak untuk mendapatkan RPN yang sama untuk risiko rendah dan tinggi sehingga mengakibatkan kedua risiko menjadi sasaran untuk mitigasi(Banghart, 2014).

Adanya perbedaan kombinasi dari faktor risiko yang mungkin akan menghasilkan nilai RPN yang sama tetapi sesungguhnya memiliki nilai esensi yang mungkin berbeda dan tersembunyi (Liu et al., 2013). Seperti penelitian yang

dilakukan oleh Patrick et al. (2005) dalam (Xiao et al., 2011), bahwa nilai *severity* dan *occurrence* adalah kunci utama yang harus digunakan dalam analisis dibandingkan parameter *detection* (D). Sebagai contoh, adanya risiko sistem rusak terdapat dua komponen RPN yang nilainya setara yaitu RPN dengan nilai 100 (RPN1 = 10(S) x 5(O) x 2(D), RPN2= 10 x 2 x 5). Dari kedua RPN tersebut dapat disimpulkan bahwa yang menjadi prioritas untuk aksi perbaikan pada dua risiko adalah sama. Namun, prioritas harus diberikan kepada risiko yang pertama, bukan yang kedua. Alasan tersebut dikarenakan nilai *occurrence* menjadi kunci utama dalam contoh permasalahan tersebut. Faktor *detection* tidak menjadi kunci dalam pengukuran yang perlu dipertimbangkan. Sedangkan, pada kasus tersebut nilai keparahannya sama-sama bernilai 10.

Menurut (Sankar & Prabhu, 2001) kelemahan dari RPN adalah metode ataupun formula yang terlalu sederhana. Kemudian adanya subjektivitas dalam skala perangkingan yang berdampak pada konsistensi hasil RPN. Sama halnya dengan peneliti lainnya, bahwa skenario hasil dari RPN bisa mendapatkan nilai kombinasi ketiga parameter dengan nilai RPN yang rendah akan tetapi memiliki potensi yang berbahaya. Sebagai contoh kasus, dalam perhitungan RPN, mode kegagalan (risiko) yang memiliki tingkat keparahan sangat tinggi, tingkat terjadi yang rendah, dan memiliki nilai deteksi yang sangat tinggi (misal: 9,3 dan 2) dengan RPN 54. Sedangkan, risiko lainnya memiliki RPN 120 dengan nilai masing parameter nya 4, 5, dan 6. Tentunya risiko yang memiliki RPN 54 seharusnya memiliki prioritas yang tinggi daripada RPN yang nilainya 120.

Disisi lain, evaluasi RPN dan prioritisasi telah dikritisi secara luas untuk FMEA tradisional. Kondisi dimana adanya tim yang memiliki pandangan berbeda dalam memberikan penilaian. Sehingga, disarankan dalam mengambil nilai rata-rata tanpa mempertimbangkan ketiga nilai dari parameter. Tim FMEA memberikan prioritas utama untuk mode kegagalan yang memiliki tingkat keparahan lebih tinggi. Dalam situasi praktis, ketiga mode kegagalan sama pentingnya dan harus dievaluasi dengan bobot yang sama dalam penentuan prioritas RPN(Sellappan et al., 2015)

Dengan analisis mode kegagalan, Tim FMEA menentukan dampak dari masing-masing kegagalan dan mengidentifikasi setiap poin kegagalan yang sangat

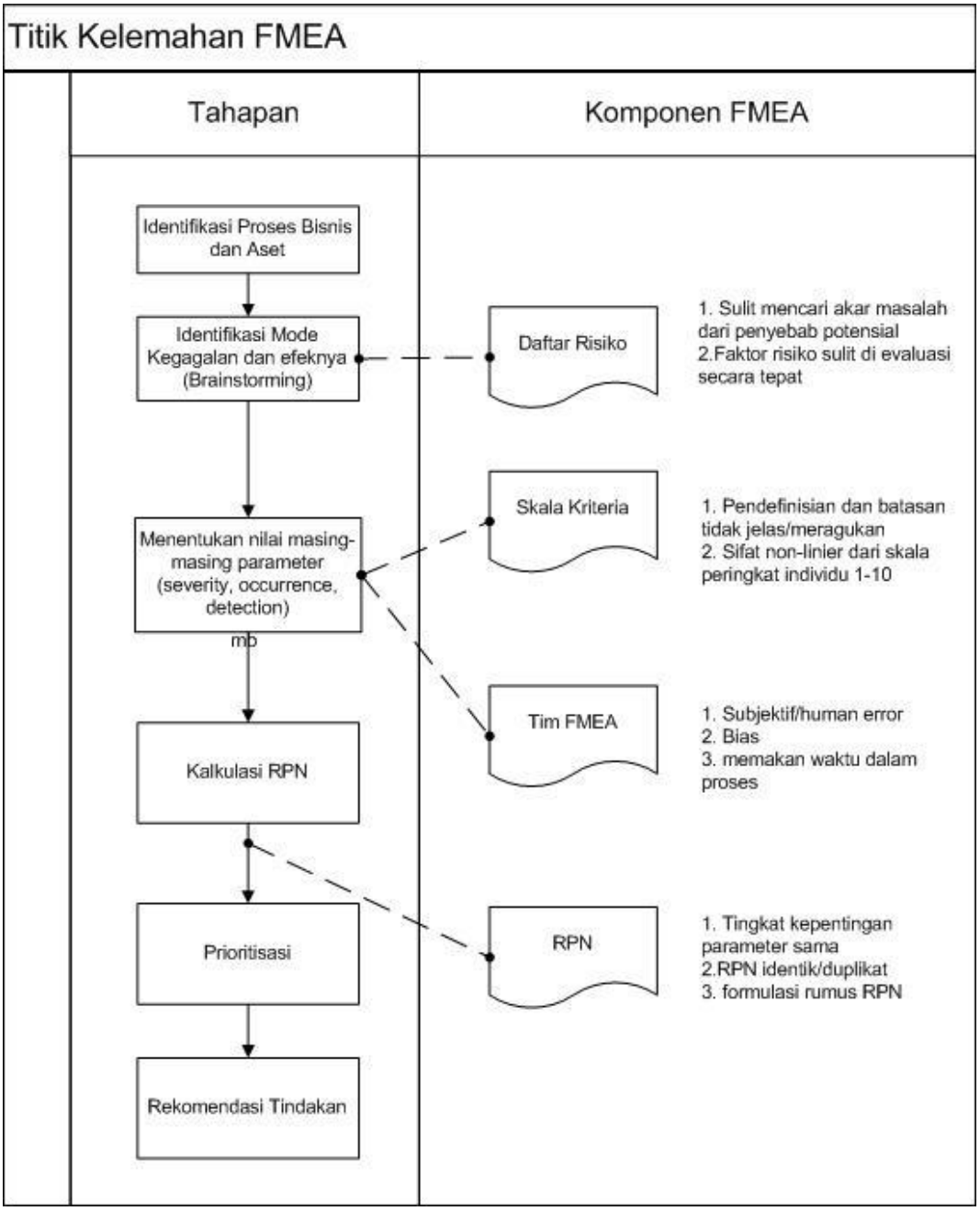
penting. Selanjutnya dilakukan pemberian peringkat masing-masing kegagalan berdasarkan dampak kegagalan yang paling kritis dan mungkin terjadi (Lipol & Haq, 2011). Hasil dari FMEA ini akan membantu para manajer dan teknisi untuk mengidentifikasi mode kegagalan, penyebabnya dan memperbaiki prosesnya (Sharma & Sharma, 2010). Tahapan FMEA yang secara umum adalah (*Software*, 2016):

1. Identifikasi potensi kegagalan dan dampaknya, tahapan ini adalah mengidentifikasi risiko dengan hasil daftar risiko. Daftar risiko tersebut terdiri dari potensi kegagalan, penyebab kegagalan, dan kontrol.
2. Menentukan tingkat keparahan (*severity*) pada masing-masing daftar risiko.
3. Menentukan nilai frekuensi sering terjadinya (*occurrence*) kegagalan pada masing-masing daftar risiko.
4. Mendeteksi kegagalan (*failure*) pada masing-masing risiko.
5. Melakukan kalkulasi *Risk Priority Number* (RPN).

Secara lebih rinci, tahapan umum tersebut lebih detail dijelaskan pada setiap tahapan berikut ini (McDermott et al., 2009):

1. Mengidentifikasi proses atau produk yang terkait.
2. Mengidentifikasi mode kegagalan (*potential failure modes*) dengan *brainstorming*.
3. Mengidentifikasi dampak dari mode kegagalan (*Potential Effect of Failure*).
4. Menentukan nilai keparahan (*severity*) dari kegagalan.
5. Menentukan nilai frekuensi sering terjadinya (*occurence*) kegagalan.
6. Menentukan peringkat deteksi (*detection*) untuk masing-masing mode kegagalan dan atau dampaknya.
7. Melakukankalkulasi nilai RPN*(Risk Priority Number*) untuk setiap dampak.
8. Melakukan prioritisasi tindakan untuk mode kegagalan.
9. Melakukan tindakan untuk mengeliminasi atau mengurangi risiko tinggi dari mode kegagalan.

Berdasarkan hasil dari literatur yang telah dibahas, diketahui bahwa letak titik kelemahan FMEA berdasarkan komponen FMEA,sehingga dapat digambarkan pada alur FMEA di bawah ini:



Gambar 4.4. Titik Kelemahan FMEA

(Sumber: Peneliti, 2018)

Berdasarkan penelitian terdahulu, dapat diketahui bahwa titik rawan yang terjadinya isu konsistensi FMEA adalah saat melakukan penilaian risiko (evaluasi risiko). Penilaian risiko dilakukan berdasarkan dokumen FMEA berupa daftar risiko dan skala kriteria sebagai panduan dalam memberikan nilai setiap parameter (*severity*, *occurrence* dan *detection*).Dokumen FMEA tersebut perlu

diperhatikan sehingga dalam penilaian risiko yang dilakukan oleh tim FMEA dapat diminimalisir isu konsistensinya.

4.3.2. Diagnosis Penyebab Inkonsistensi

Dalam mengevaluasi FMEA dilakukan dengan melihat perolehan nilai RPN. RPN tidak hanya terdiri dari tingkat keparahan dan tingkat terjadi, akan tetapi juga dari tingkat kemungkinan deteksi risiko. Ketidakpastian nilai RPN dapat diestimasi dari ketidakpastian dari masing-masing nilai yang diberikan pada ketiga parameter tersebut(Cameron et al., 2017). Oleh karena itu, penyebab inkonsistensi dapat dilihat berdasarkan dokumen FMEA yang telah dibentuk untuk dilakukan pengukuran oleh tim FMEA.

Kelemahan dalam penggunaan FMEA juga terbukti berdasarkan hasil dari siklus *action research* yang pertama. Isu konsistensi yang dikemukakan oleh peneliti tersebut terbukti dengan adanya perbedaan nilai RPN yang didapatkan dari dua tim yang berbeda pada studi kasus yang sama (Estorilio & Posso, 2010), (Barends et al., 2012), (Oldenhof et al., 2011), (Gary Teng et al., 2006). Adapun hasil perolehan RPN pada tim pertama adalah 3 risiko berada pada level *very high,* sedangkan pada tim kedua adalah 6 risiko berada pada level *very high.* Terdapat kesenjangan dengan 3 RPN yang tidak berbeda pada kedua RPN hasil tim tersebut.

Komponen dokumen FMEA yang telah dikritisasi berdasarkan fakta lapangan yang diperoleh bahwa faktor perbedaan dari jawaban ketiga parameter (*security,detection,occurrence*) menyebabkan perbedaan nilai RPN pada daftar risiko yang sama. Kedua tim menggunakan dokumen yang sama dan skala yang sama, dan hasil nilai RPN yang diperoleh berbeda. Hal inilah yang menjadi *gap* antara kedua tim. Berdasarkan kelemahan yang diidentifikasi, perbedaan nilai tersebut karena dari daftar risiko yang memiliki banyak variabel risiko sehingga menyebabkan sulitnya mengevaluasi risiko tersebut secara tepat. Kemudian, sulitnya mencari akar permasalahan seperti sumber ancaman yang tepatdikarenakan kelemahan FMEA yang tidak memiliki prosedur terkait penentuan skala risiko yang efektif dan efisien. Seperti hasil analisis *gap* yang dilakukan dari segi pelatihan, informan telah mendapatkan pelatihan terkait

SISKOHAT setiap tahunnya yang diadakan oleh Pusat. Dari kedua tim, tentunya pemahaman terhadap proses bisnis dan seluk-beluk SISKOHAT sangat berpengaruh pada pemberian informasi untuk mendukung pemberian nilai risiko. Pada Bidang Penyelenggaraan haji dan umrah juga belum pernah dilakukan pengukuran risiko Teknologi Informasi sehingga pengetahuan informan terhadap risiko masih kurang.

Skala umum FMEA yang digunakan adalah skala 10 dan setiap parameter memiliki tingkat kepentingan yang sama. Skala dengan rentangan nilai yang panjang membuat pendefinisian risiko sulit ditentukan angka yang tepat. Hal ini dapat dilihat pada kedua tim, butuh waktu lebih dari dua jam dalam penyelesaiannya. Sehingga, dari kelemahan tersebut penyebabnya adalah tidak adanya estimasi waktu yang jelas sehingga isu subjektivitas akan lebih besar jika waktu penentuan lebih lama. Perlu adanya estimasi waktu dan pembagian tugas yang jelas (McDermott et al., 2009). Tidak lebih dari 90 menit dalam melakukan evaluasi risiko (Estorilio & Posso, 2010).

Permasalahan umum yang ada pada FMEA berdasarkan pengalaman (Gary Teng et al., 2006), bahwa kurangnya informasi yang rinci pada fungsi produk atau sistem, mode potensial kegagalan, potensi dampak dari kegagalan, potensi penyebab kegagalan, dan perancangan kontrol yang ada. Dengan kurangnya informasi ini menyebabkan kesalahpahaman, kebingungan atau ketidakpastian dalam pendefinisian risiko. Hal ini sesuai dengan hasil dari siklus *action research* pertama yaitu tim pertama cenderung lebih banyak memakan waktu dalam memberikan pemahaman akan risiko yang akan berdampak dari segi keparahan, deteksi dan tingkat terjadinya. Tim pertama lebih cenderung pasif dalam memberikan penilaian risiko. Sedangkan tim kedua, penilaian risiko berlangsung lebih atraktif karena informan memberikan informasi yang lebih detail sehingga dalam penilaian risiko lebih cepat terselesaikan. Data tersebut tidak menyediakan indikasi yang jelas dimana kondisi kegagalan atau proses kegagalan terjadi, ataupun menyediakan informasi yang jelas tentang penyebab kegagalan tersebut. Pada banyak kasus, data tidak tersedia sehingga berdasarkan pada pengetahuan dan pengalaman pegawai dalam organisasi dalam memprediksi tingkat nilai ketiga parameter(Banghart, 2014).

Subjektifitas individual dan bias juga berdampak pada dinamika tim. Belum adanya prosedur ataupun panduan FMEA dalam menentukan anggota tim serta kriteria anggota tim yang dibutuhkan. Hal ini menjadi penting karena kesalahan pendefinisian risiko bergantung pada pengalaman anggota tim dalam menganalisis kegagalan dan familiarnya sistem bagi anggota serta bias kognitif yang diketahui. Dengan demikian, sangat adanya kemungkinan kesalahan manusia. Situasi ini sering terjadi bila sedikit data mengenai kejadian dan efek kegagalan diketahui, sehingga memerlukan subjektivitas(Banghart, 2014). Dari hasil yang tidak konsisten disebabkan oleh subjektifitas ini sehingga perlu adanya strategi untuk mengatasi subjektifitas tim FMEA dalam melakukan penilaian risiko.

Menurut Odenholf, et al (2011), paling sedikit ada dua teknisi ahli yang termasuk dalam tim FMEA untuk menyeimbangkan perbedaan individu yang signifikan dalam keputusan risiko yang krusial. Jumlah tim yang ganjil membantu dan memudahkan dalam proses perhitungan *voting.*KelemahanFMEA yang memakan waktu dalam proses dapat diminimalkan dengan tim yang multidisiplin sehingga memahami dengan baik proses yang dianalisa(Jain, 2017).Strategi tersebut telah sesuai dengan *action research* pertama dengan melibatkan praktisi TI dan pegawai, dengan jumlah anggota tim adalah ganjil.

Tim FMEA memberikan prioritas teratas untuk risiko yang memiliki dampak yang tinggi. Dalam praktiknya, terkadang ketiga dari parameter memiliki tingkat kepentingan yang setara dan harus adanya evaluasi dengan bobot nilai yang sama dalam prioritisasi RPN (Sellappan et al., 2015). Hasil risiko dengan FMEA yang tidak akurat akan berdampak pada keseluruhan proses FMEA. *Error* tersebut secara spesifik berdampak pada praktisi yang sedang menentukan mode kegagalan diprioritaskan dan membangun strategi mitigasinya. Pada praktiknya hal ini sulit diukur akuratnya dan harus adanya keseimbangan teori dan aplikasi praktik terhadap perhitungan risiko menggunakan FMEA. Penting untuk dipahami bahwa sesungguhnya ketidakpastian juga berasal dari analisis FMEA. Kemungkinan yang tidak pasti dari kegagalan sistem dan perbaikannya, hal ini berdampak pada *error* selama proses penilaian risiko(Banghart, 2014).

Berdasarkan penjelasan yang telah dipaparkan diatas, dapat dituliskan penyebab inkonsistensi yang diselaraskan dengan kelemahan proses FMEA pada penelitian ini adalah:

Tabel 4.12. Penyebab Inkonsistensi

No	Kelemahan	Penyebab
1	Sulit mencari akar masalah dari penyebab potensial	Pendefinsian sumber ancaman yang kurang tepat.
2	Faktor risiko sulit dievaluasi secara tepat	Banyaknya variasi skenario yang berpengaruh pada hasil RPN yang identik.
3	Pendefinisian dan batasan skala kriteria tidak jelas dan meragukan	Tidak ada prosedur khusus penentuan skala kriteria.
4	Sifat non-linier dari skala peringkat individu 1-10	Skala 1-10 membuat tim berfikir lebih lama dalam menentukan skala yang tepat karena banyaknya pertimbangan angka yang tepat.
5	Subjektif/*human error*	1. Belum ada panduan mengenai anggota tim 2. Pengalaman 3. Pengetahuan
6	Bias	
7	Memakan waktu dalam proses	Tidak adanya batas waktu dalam penilaian
8	Tingkat kepentingan parameter sama	Tidak ada bobot nilai/ variabel yang menjadi kunci utama yang harus digunakan dalam analisis.
9	RPN identik/duplikat	Banyaknya variasi kombinasi dapat menyebabkan samanya nilai RPN.Banyaknya variasi kombinasi nilai RPN(max=1000)
10	Formulasi rumus RPN	Rumus yang terlalu sederhana karena menganggap sama setiap tingkat kepentingannya.

Penyebab yang telah didefinisikan tersebut menjadi inputan dalam melakukan sintesis kerangka FMEA yang ditingkatkan. Dengan memperbaiki penyebab inkonsistensi FMEA seharusnya akan memberikan hasil yang lebih konsisten daripada yang sebelumnya.

4.4.3. Sintesis Kerangka FMEA (*Improvement*)

Kelemahan FMEA telah didefinisikan sebelumnya, merupakan kritikan dari penelitian terdahulu terkait permasalahan yang ada selama ini dalam mengevaluasi risiko. Kelemahan-kelemahan tersebut tentunya dapat diminimalisir dengan melihat usulan perbaikan berdasarkan penelitian terdahulu yang telah melakukan uji coba ataupun eksperimen dalam meningkatkan FMEA yang efektif. FMEA yang efektif tersebut tergantung pada pemahaman dari fundamental dan prosedur FMEA, menentukan FMEA yang benar dan tim FMEA (Sellappan et al., 2015).

Berdasarkan hasil analisis kesenjangan pada siklus pertama, diketahui bahwa adanya kesenjangan dari faktor perbandingan jawaban ketiga parameter, orang (tim FMEA), waktu penyelesaian, pelatihan, pengetahuan, dan sejarah terjadinya risiko (*failure history*). Perbandingan dari faktor tersebut membandingkan antara *current practice* dan *best practice* yang merujuk pada penelitian sebelumnya. Perbaikan yang dilakukan pada siklus kedua ini merupakan integrasi temuan lapangan dan penelitian terdahulu. Pada subbab sebelumnya telah dibahas titik kelemahan dan penyebab inkonsistensi metode FMEA. Dari kedua hal tersebut, diberikan rekomendasi solusi yang tergambar pada tabel di bawah ini:

Tabel 4.13. Keselarasan kelemahan, penyebab, dan rekomendasi solusi

No	Kelemahan	Penyebab	Rekomendasi Solusi
1	Sulit mencari akar masalah dari penyebab potensial	Pendefinsian sumber ancaman yang kurang tepat.	Memberikan informasi kategori sumber ancaman dalam *risk register*. Mencari akar masalah dari penyebab dampak yang jarang

2	Faktor risiko sulit dievaluasi secara tepat	Banyaknya variasi skenario yang berpengaruh pada hasil RPN yang identik.	terlihat dalam sebuah komponen sistem (Cameron et al., 2017). Sehingga, kategori sumber ancaman tersebut dapat meminimalisir ambiguitas dalam pemahaman *failure.*
3	Pendefinisian dan batasan skala kriteria tidak jelas dan meragukan	Tidak ada prosedur khusus penentuan skala kriteria.	Membatasi ukuran variabel parameter (Skala) dapat menjadikan FMEA menjadi metode yang lebih cepat, menjadi lebih efektif serta menghasilkan hasil yang kuat. (Paciarotti et al., 2014). Mengkategorikan skala risiko tingkat keparahan kedalam 3 kategori jenis risiko yaitu risiko pelayanan/operasional, perhatian media dan regulasi.
4	Sifat non-linier dari skala peringkat individu 1-10	Skala 1-10 membuat tim berfikir lebih lama dalam menentukan skala yang tepat karena banyaknya pertimbangan angka yang tepat.	
5	Subjektif/*human error*	1. Belum ada panduan mengenai anggota tim 2. Pengalaman 3. Pengetahuan	1. Menurut hasil penelitian Odenholf, et al (2011) yaitu paling sedikit ada dua teknisi ahli yang termasuk dalam tim FMEA untuk menyeimbangkan perbedaan individu yang signifikan dalam keputusan risiko yang krusial. Jumlah tim yang ganjil membantu dan memudahkan dalam proses perhitungan *voting*.Kriteria anggota tim FMEA didefinisikan sebelum melakukan pembentukan tim. 2. Adanya pelatihan terkait metode FMEA dan perkenalan terhadap risiko TI (Estorilio &
6	Bias		

			Posso, 2010).
7	Memakan waktu dalam proses	Tidak adanya batas waktu dalam penilaian	Pondasi dari FMEA adalah anggota tim dan hasil masukan dari proses FMEA dan perlu adanya estimasi waktu dan pembagian tugas yang jelas (McDermott et al., 2009). Tidak lebih dari 90 menit(Estorilio & Posso, 2010).
8	Tingkat kepentingan parameter sama	Tidak ada bobot nilai/ variabel yang menjadi kunci utama yang harus digunakan dalam analisis.	Menurut Patrick et al. (2005) dalam (Xiao et al., 2011), bahwa nilai *severity* dan *occurrence* adalah kunci utama yang harus digunakan dalam analisis dibandingkan parameter *detection* (D).
9	Formulasi rumus RPN	Rumus yang terlalu sederhana karena menganggap sama setiap tingkat kepentingannya.	
10	RPN identik/duplikat	Banyaknya variasi kombinasi dapat menyebabkan samanya nilai RPN.Banyaknya variasi kombinasi nilai RPN(max=1000)	Membatasi ukuran variabel parameter (Skala) dapat menjadikan FMEA menjadi metode yang lebih cepat, menjadi lebih efektif serta menghasilkan hasil yang kuat. (Paciarotti et al., 2014)

Penjelasan mendalam terkait rekomendasi solusi dalam tahapan yang FMEA yang disintesis terdapat dalam metodologi kerangka FMEA yang diperbaiki (*FMEA Improvement*) seperti di bawah ini:

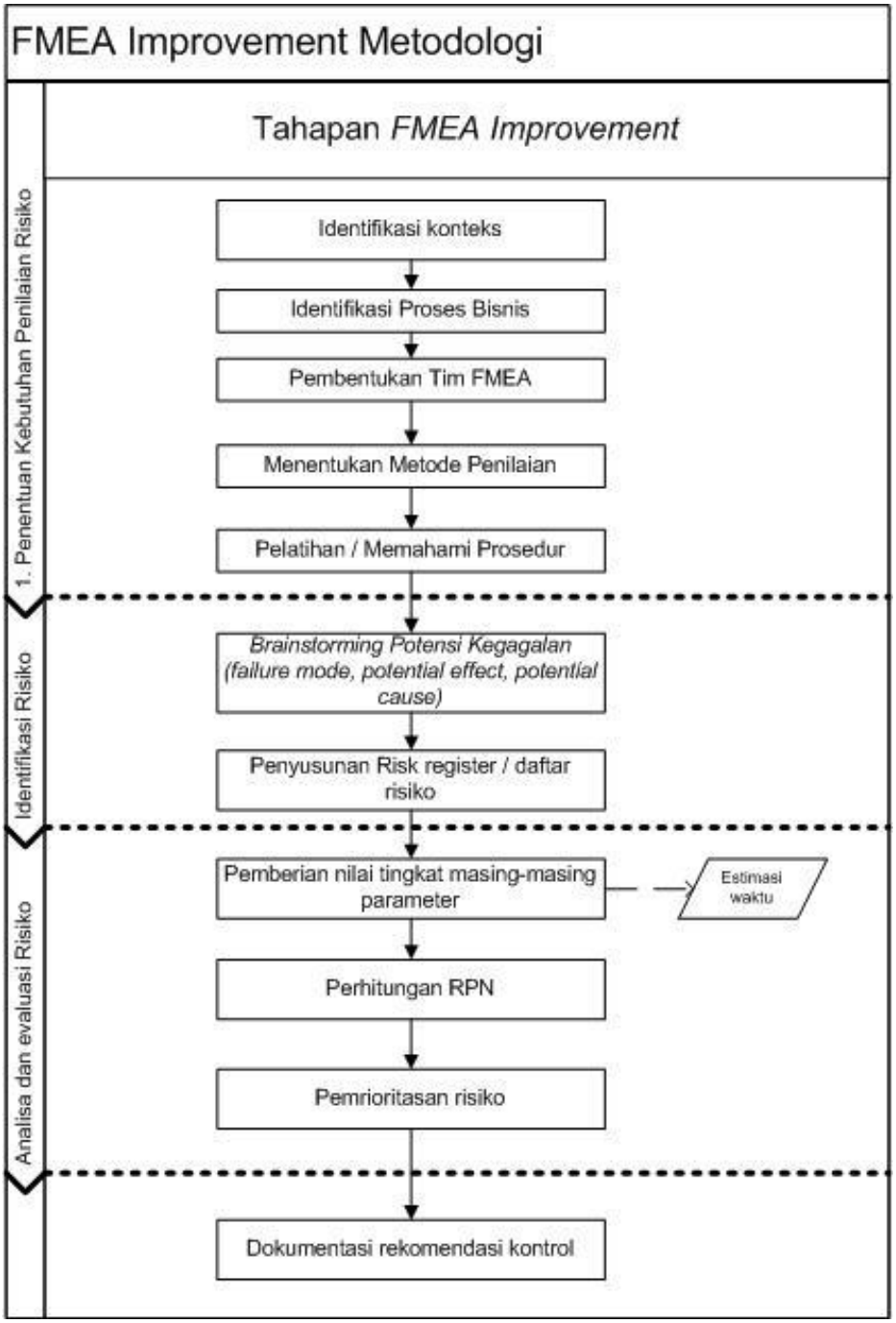
Tabel 4.14. Kerangka FMEA *Improvement*

Tahapan	**Nama Tahapan**	**Bagian Tahapan**	**Keterangan**	**Acuan Referensi**
1	Penentuan Kebutuhan Penilaian Risiko	Identifikasi Konteks	Pendefinisian target sistem yang digambarkan dan identifikasi aset.	(Desy et al., 2014)
		Identifikasi Proses Bisnis	Memahami alur proses bisnis pada objek.	(McDermott et al., 2009)
		Pembentukan tim FMEA	Menentukan pihak yang terkait dalam penilaian risiko.	(Oldenhof et al., 2011), (Alberts & Dorofee, 2002)
		Menentukan Metode Penilaian	Skala kriteria dan desain dokumen FMEA yang telah diperbaiki.	(Carlson, 2014)
		Pelatihan & Pemahaman Prosedur	Melakukan pelatihan kepada tim dan memberikan pemahaman prosedur penggunaan metode FMEA yang telah disintesis.	(Estorilio & Posso, 2010), (Carlson, 2014)
2	Identifikasi Risiko	*Brainstorming* Potensi Kegagalan (*failure mode, potential effect, potential cause*)	Dalam OCTAVE diketahui sebagai identifikasi aset kritis, membangun profil berbasis ancaman, profil aset berbasis ancaman, identifikasi	(Whitman & Mattord, 2012), (Alberts & Dorofee, 2002)

			kelemahan infrastruktur.	
		Penyusunan *risk register* / daftar risiko	Mensintesis hasil *brainstorming* ke dalam pentabelan dokumen FMEA.	(Cameron et al., 2017), (McDermott et al., 2009), (Stamatis, 2003), (Security, 2008), (Lai & Chin, 2014)
3	Analisa dan evaluasi Risiko	Pemberian nilai tingkat pada masing-masing parameter	Memberikan nilai frekuensi terjadinya risiko, nilai keparahan risiko, dan nilai deteksi risiko.	(McDermott et al., 2009), (Stamatis, 2003)
		Perhitungan RPN	Melakukan perhitungan sesuai dengan formulasi RPN.	
		Pemrioritasan risiko	Mengurutkan nilai RPN dari yang besar hingga paling kecil dan membuat level risiko.	
4	Rekomendasi Kontrol	Dokumentasi rekomendasi kontrol	Risiko yang akan dievaluasi dan dimitigasi dimasukkan kedalam dokumentasi rekomendasi kontrol.	(Lai & Chin, 2014)

Sumber: Olahan Peneliti, 2018

Berdasarkan tabel diatas, alur aktivitas dalam FMEA yang telah disintesis adalah sebagai berikut:



Gambar 4.5. Alur FMEA yang Disintesis

Adapun penjelasan setiap tahapan adalah sebagai berikut:

1. Identifikasi Konteks

Kegiatan dalam mengidentifikasi konteks adalah menentukan ruang lingkup penilaian risiko, dimana target sistem yang digambarkan dan identifikasi aset (Misra et al, 2007) dalam (Lai & Chin, 2014). Pengidentifikasian aset TI

menurut (Desy et al., 2014) menentukan objek sistem atau teknologi informasi yang ingin diukur risikonya. Penentuan aset kritis dikategorisasikan berdasarkan *hardware, software, people, data,* dan *network* (Desy et al., 2014).

2. Identifikasi Proses Bisnis

Kegiatan dalam tahapan ini adalah memahami alur proses bisnis pada objek. Dengan adanya tahapan ini membantu dalam memahami kinerja sistem dan alur proses bisnis yang sedang berjalan (McDermott et al., 2009). Analisis proses bisnis juga membantu dalam menyatukan pemikiran kepada tim FMEA sehingga penilaian yang didapatkan lebih akurat.

3. Pembentukan Tim FMEA

Kegiatan dalam tahapan ini adalah menentukan pihak yang terkait dalam penilaian risiko.Berikut ini prosedur dalam pembentukan tim FMEA:

a. Ukuran tim : Jumlah tim yang ganjil membantu dan memudahkan dalam proses perhitungan voting. Minimal tim berjumlah 3 orang.(Alberts & Dorofee, 2002)
b. Anggota tim : Menurut hasil penelitian Odenholf, et al (2011) yaitu paling sedikit ada dua teknisi ahli yang termasuk dalam tim FMEA untuk menyeimbangkan perbedaan individu yang signifikan dalam keputusan risiko yang krusial. FMEA yang memakan waktu dalam proses dan membutuhkan tim yang multidisiplin sehingga memahami dengan baik proses yang dianalisa(Jain, 2017). Kriteria lainnya yang perlu diperhatikan adalah (Alberts & Dorofee, 2002):
    1) Orang yang mengetahui tipe-tipe informasi yang berhubungan dengan aset yang terdapat dalam organisasi.
    2) Orang yang mengetahui cara mendapatkan informasi aset tersebut.
    3) Orang yang berkomitmen untuk menyediakan waktu untuk pengukuran risiko.
    4) Orang yang telah berada pada jabatannya minimal satu tahun.
    5) Memiliki otoritas untuk memilih dan memberikan perintah kepada staff untuk mengukur risiko (khusus : level manajemen).

c. Ketua tim: Seorang ketua tim harus mengontrol dan mengkoordinasi jalannya proses pengukuran risiko. Adapun hal yang harus di koordinasikan adalah (McDermott et al., 2009):
    1) Mengatur dan memfasilitasi pertemuan termasuk jadwal dan dokumen FMEA yang akan diisi.
    2) Memastikan tim yang bersangkutan hadir.
    3) Memastikan suksesnya pengukuran risiko hingga selesai.

4. Menentukan Metode Penilaian

Penentuan metode penilaian yaitu menentukan desain dokumen FMEA beserta skala kriteria yang digunakan dalam pengukuran risiko(Carlson, 2014). Berikut merupakan modifikasi yang dilakukan pada metode penilaian:

1. Memberikan informasi kategori sumber ancaman(*people, process,* dan *technology*) dalam *risk register*. Mencari akar masalah dari penyebab dampak yang jarang terlihat dalam sebuah komponen sistem (Cameron et al., 2017). Kategori sumber ancaman tersebut dapat meminimalisir ambiguitas dalam pemahaman *failure.*
2. Menghilangkan *detection* dalam perhitungan risiko. Adapun justifikasi penghilangan variabel *detection* adalah:
    1) Seperti penelitian yang dilakukan oleh Patrick et al. (2005) dalam (Xiao et al., 2011), bahwa nilai *severity* dan *occurrence* adalah kunci utama yang harus digunakan dalam analisis dibandingkan parameter *detection* (D).
    2) *Detection* membutuhkan alat/*tools* sedangkan pada studi kasus yang dituju tidak adanya *toolsdetection*, seperti adanya *event monitoring tools.* Dengan menghilangkan *detection* mengurangi usaha tim dalam mengukur risiko dan mempercepat proses pengukuran sehingga diasumsikan kurang dari 90 menit.
    3) Merujuk pada ISO 31000, bahwa variabel yang penting dalam pengukuran risiko adalah probabilitas=*occurrence* dan konsekuensi = *severity.*

3. *Potential Effect of Failure* menggunakan kategori skala kriteria yaitu dampak terhadap pelayanan/operasional, perhatian media, dan regulasi. Berikut ini adalah desain dokumen FMEA yang telah ditingkatkan:

Code	***Critical Assets***	**(impact)** ***Potential Failure Modes (s)***	***Potential Effect(s) of Failure***	***SEV***	**(threat)** ***Potential Cause(s) / Mechanism (s) of Failure***	***Source of Threat***	***OCC***	***Current Compensanting Controls*** **(Compensate Vulnerability)**		***RPN***
								Preventive Control	***Detective Control***	
<kode aset>	<nama aset>	<dampak akhir jika terjadinya ancaman>	Dampak pada kategori skala kriteria	1	Ancaman	*<people, process, technology>*	1	Pencegahan	*Monitoring*	1

Berdasarkan titik kelemahan FMEA bahwa skala kriteria 1-10 merupakan penyebab lamanya tim FMEA dalam menentukan nilai yang tepat untuk risiko yang diidentifikasi.Banyaknya variasi kombinasi nilai RPN(max=1000). Banyaknya variasi kombinasi dapat menyebabkan samanya nilai RPN dan memakan waktu yang lama. Seperti penjelasan pada subbab sebelumnya, waktu yang lama akan memberikan dampak pada isu bias dan subjektifitas dalam pemilihan nilai yang tepat. Membatasi ukuran variabel parameter (Skala) dapat menjadikan FMEA menjadi metode yang lebih cepat, menjadi lebih efektif serta menghasilkan hasil yang kuat(Paciarotti et al., 2014). Pada penelitian ini, menggunakan skala 1-5.

a. Kriteria Skala Tingkat Keparahan / *Severity*

Skala	**Level Skala**	**Tingkat keparahan terhadap**		
		Pelayanan/ operasional	**Perhatian media**	**Regulasi**
1	Sangat Kecil	Tidak Berdampak	Tidak berdampak	Tidak Berdampak
2	Kecil	Dampak dapat	Potensi	Percobaan

		diabaikan	menjadi sorotan publik	akses ke SISKOHAT.
3	Sedang	Kegiatan operasional ataupun kinerja terhambat.	Pemberitaan negatif pada media massa	Sistem operasional ditembus oleh *hacker/cracker*
4	Besar	Pelayanan terhadap calon jemaah terganggu lebih dari 24 jam.	Ekspos utama (di media massa) lebih dari satu hari	Investigasi oleh pihak berwajib atau *regulatory*
5	Sangat Besar	Ketidaknyaman an yang berarti/ keresahan timbul dari seluruh calon jemaah.	Menjadi perhatian pemerintah / kehilangan kepercayaan publik	Kegagalan sistem menyeluruh / sistem secara total tidak berfungsi, kerugian

b. Kriteria Skala Tingkat Terjadi / *Occurrence*

Skala	**Level Skala**	**Tingkat Terjadi**
1	Sangat Tidak Mungkin	Dapat diabaikan
2	Mungkin	Kecil kemungkinan terjadi
3	Kadang-kadang	Kemungkinan terjadi sedang / Bisa Terjadi
4	Hampir Pasti	Kemungkinan besar terjadi
5	Pasti Terjadi	Akan terjadi (dalam segala situasi)

c. Level Risiko

Inherent Risk		Risk Level	Action Plan
1-5	Low	Diterima	-
6-10	Low to Medium	Diterima	-
11-15	Medium	Diterima	-
16-20	Medium to High	Tidak Diterima	Dihilangkan, dikurangi, dipindahkan
21-25	High	Tidak Diterima	Dihilangkan, dikurangi, dipindahkan

5. Pelatihan/Memahami Prosedur

Adanya pelatihan terkait metode FMEA dan perkenalan terhadap risiko TI (Estorilio & Posso, 2010). Pelatihan berguna memahami prosedur digunakan untuk menjelaskan detail langkah-langkah yang perlu dilakukan dalam menganalisis dan menilai risiko menggunakan metode FMEA. Kemudian, dengan adanya pelatihan menyatukan persepsi dan pengetahuan dari anggota tim terhadap risiko TI yang akan dinilai(Carlson, 2014).

6. Brainstorming Potensi Kegagalan (*failure mode, potential cause, potential effect*)

Menurut tahapan OCTAVE, tahapan awal yang dilakukan untuk mengukur risiko adalah pendefinisian aset kritis. Identifikasi aset kritis dilakukan untuk mengetahui aset teknologi informasi yang dimiliki oleh studi kasus yang akan diteliti. Sehingga, dengan mengidentifikasi aset kritis dapat didefinisikan dan membentuk daftar risiko yang akan dianalisis. Identifikasi aset kritis dengan cara mengumpulkan data-data terkait dengan kondisi eksisting dari studi kasus. Tahapan dalam mengidentifikasi kondisi eksisting tersebut adalah dengan membangun profil ancaman berbasis aset (identifikasi aset kritis, identifikasi kebutuhan keamanan aset, identifikasi ancaman, identifikasi keamanan yang sudah diterapkan, dan identifikasi kelemahan organisasi), kemudian dilakukan identifikasi kerentanan infrastruktur (identifikasi komponen utama, identifikasi

kelemahan teknologi yang sudah ada) (Alberts & Dorofee, 2002). Pada tahapan ini dilakukan wawancara dan observasi.

7. Penyusunan *Risk Register* atau daftar risiko

Kegiatan dalam tahapan ini adalah memasukkan hasil dari *brainstorming* potensial kegagalan yang diperoleh pada tahapan sebelumnya ke dalam dokumen FMEA yang telah disediakan formatnya. Sehingga, dihasilkan daftar risiko atau *risk register* yang siap digunakan pada tahapan selanjutnya.

8. Pemberian nilai tingkat masing-masing parameter

Pada tahapan ini dilakukan pengukuran masing-masing parameter yaitu *severity* dan *occurence.* Pengukuran mengacu pada desain dokumen FMEA yang telah disusun. Pondasi dari FMEA adalah anggota tim dan hasil masukan dari proses FMEA dan perlu adanya estimasi waktu dan pembagian tugas yang jelas (McDermott et al., 2009) dan tidak lebih dari 90 menit(Estorilio & Posso, 2010).

9. Perhitungan RPN

Tahapan ini mengkalkulasikan hasil masing-masing daftar risiko dengan mengkalikan nilai *severity* dan nilai *occurrence.*

10. Pemrioritasan Risiko

Tahapan ini melakukan pengurutan nilai RPN dari yang terbesar hingga terkecil. Kemudian, langkah selanjutnya adalah menentukan level risiko. Level risiko menentukan seberapa besar risiko tersebut dalam organisasi dan membutuhkan rekomendasi aksi. Penggolongan risiko berdasarkan level risiko ini menentukan risiko tersebut dapat diabaikan/diterima, dihilangkan sumber ancamannya, dimitigasi untuk sebagai pencegahan terjadinya risiko, atau adanya pengawasan terhadap sumber ancaman terjadinya risiko.

11. Dokumentasi rekomendasi kontrol

Tahapan ini sebagai dokumentasi untuk evaluasi risiko pada keberlanjutan penilaian risiko yang telah menjalankan rekomendasi kontrol.

4.4. Validasi Pakar

4.4.1. Profil Pakar

Penelitian ini menggunakan validasi bertingkat. Untuk validasi dokumen FMEA pada siklus pertama, dilakukan oleh dua orang praktisi TI yang dijelaskan pada siklus *action research* pertama. Sedangkan pada validasi dokumen FMEA yang disintesis (FMEA *Improvement*) dilakukan oleh pakar yang telah mendapatkan sertifikasi di bidang Tata Kelola TI. Validasi pakar berguna sebagai pengesahan bahwa instrumen penelitian yang digunakan dan kerangka FMEA yang ditingkatkan telah sesuai baik secara teoritis maupun praktisnya. Pakar yang melakukan validasi memiliki kualifikasi seperti memiliki pengetahuan dan keahlian di bidang manajemen risiko Teknologi Informasi serta memiliki pengalaman kerja dalam menggunakan FMEA. Berikut merupakan profil pakar yang memvalidasi FMEA yang disintesis:

Tabel 4.15. Profil Pakar

Profil Pakar	
Nama:	Aresto Yudo, S.Kom, M.Sc, CGEIT, CISA
Pekerjaan:	*Manager Consultant*
Bidang Keahlian:	1. Manajemen Risiko 2. Tata Kelola TI 3. Audit TI
Pengalaman Pekerjaan:	1. *Lead Consultant*: *IT Risk Management* – BUMN Sektor Maritim (2016) 2. *Project Manager*: *IT Risk Management* – Perusahaan Sektor Perbankan (2011) 3. *Lead Consultant*: *IT Governance Assessment – Self Regulated Organization* Indonesia (2008) 4. *Team Leader*: *IT Audit* – Berbagai Jenis Industri (2005-2016)
Keanggotaan Organisasi Profesional:	1. *Information Systems Audit and Control Association* (ISACA) 2. *The Open Group* 3. AISINDO
Sertifikasi:	1. CGEIT *(Certified in the Governance Enterprise of Information Technology)* 2. CISA *(Certified of Information Sytems Auditor)*

4.4.2. Hasil Validasi Pakar

Validasi pakar memberikan penilaian kesesuaian desain dokumen FMEA dengan memberikan ceklis pada setiap tahap atau elemen FMEA yang disintesis. Kemudian, Pakar juga memberikan pernyataan bahwa dokumen FMEA yang disintesis telah sesuai dengan praktis maupun teoritis. Hasil validasi yang dilakukan oleh pakar meliputi, (i) Kesesuaian tahapan/elemen FMEA *improvement,* (ii) kecukupan metodologi FMEA *improvement,* dan (iii) relevansi rancangan mekanisme terhadap praktik-praktik di organisasi.Berikut ini adalah hasil dari validasi yang meliputi keempat poin validasi:

Tabel 4.16. Kesesuaian desain dokumen FMEA dan skala kriteria

No	Elemen FMEA	Ya	Tidak	Keterangan (jika tidak sesuai)
1	Identifikasi Konteks	✓		
2	Identifikasi Proses Bisnis	✓		
3	Pembentukan tim FMEA	✓		
4	Menentukan Metode Penilaian	✓		
5	Pelatihan & Pemahaman Prosedur	✓		
6	*Brainstorming* Potensi Kegagalan (*failure mode, potential effect, potential cause*)	✓		
7	Penyusunan *risk register* / daftar risiko	✓		
8	Pemberian nilai tingkat pada masing-masing parameter (kontrol: estimasi waktu <90 menit)	✓		
9	Perhitungan RPN	✓		
10	Pemrioritasan risiko	✓		
11	Dokumentasi rekomendasi kontrol	✓		

Berdasarkan hasil tersebut, 11 elemen pada tahapan FMEA yang disintesis telah sesuai dan cukup. Poin kedua terkait dengan pendapat pakar terhadap kecukupan metodologi FMEA yang disintesis. Pada poin ini pakar memberikan masukan untuk mengkategorikan *potential effect* sesuai dengan skala kriteria tingkat keparahan. Hal ini perlu dilakukan agar selarasnya parameter pengukuran risiko. Kemudian, pakar memberikan pandangan bahwa membuat nama kolom dengan bahasa indonesia agar dapat dan mudah dimengerti oleh tim yang

mengukur risiko. Seluruh masukan tersebut telah dipenuhi oleh peneliti untuk selanjutnya dapat digunakan dalam implementasi FMEA *improvement.*

Menurut pakar, penelitian ini mengidentifikasi subjektivitas pelaku evaluasi risiko sebagai penyebab utama inkonsistensi dari metode FMEA tradisional. Berdasarkan observasi yang dilakukan, penelitian ini kemudian mensintesis perbaikan metodologi FMEA dengan beberapa langkah yang mengurangi faktor subjektivitas dalam setiap tahapan. Pada poin ketiga, pakar menyatakan bahwa tahapan dalam perbaikan metodologi FMEA yang dihasilkan dari penelitian ini sudah sesuai dengan praktik pada umumnya.

4.5. Implementasi *Action research* 2

4.5.1. Identifikasi Konteks

Identifikasi konteks adalah menentukan ruang lingkup penilaian risiko dimana target sistem yang digambarkan dan identifikasi aset (Misra et al, 2007) dalam (Lai & Chin, 2014). Pengidentifikasian aset TI menurut (Desy et al., 2014) dengan menentukan objek sistem atau teknologi informasi yang ingin diukur risikonya. Berikut ini adalah identifikasi konteks yang didapatkan:

1. Tujuan

Penetapan tim risiko bertujuan untuk memastikan tim risiko yang melakukan penilaian risiko menggunakan metode FMEA *Improvement* telah memahami dan berpengalaman dalam penggunaan metode FMEA, sehingga mengurangi tingkat hasil yang tidak konsisten dalam melakukan penilaian risiko.

2. Ruang Lingkup Pengukuran Risiko

Ruang lingkup penetapan tim risiko adalah pihak-pihak yang terlibat dalam kegiatan manajemen risiko pada aset kritis instansi dalam penggunaan teknologi informasi menggunakan metode FMEA *Improvement*.

3. Indikator Kinerja

Kesesuaian waktu pelaksanaan prosedur dengan jadwal yang telah ditetapkan oleh pembuat prosedur (instansi). Koordinator dilakukan berdasarkan kontrol dari peneliti.

4. Objek Pengukuran risiko TI

Objek pengukuran risiko TI adalah Sistem Komputerisasi Haji Terpadu pada Bidang Penyelenggaraan Haji dan Umrah, Kantor Wilayah Kementerian Agama Provinsi Riau.

5. Komponen Aset Kritis TI

Berikut ini adalah kategori asset kritis dikategorisasikan berdasarkan *hardware, software, people, data,* dan *network* (Desy et al., 2014).

Tabel 4.17. Komponen aset kritis

Kategori Aset	**Aset Kritis**	**Deskripsi**
Hardware	*Server*	Menyimpan data-data yang ada pada SISKOHAT.
	Komputer/PC	Perangkat komputer yang digunakan untuk melakukan pengolahan data jemaah haji yang hanya dapat diakses pada komputer instansi di Bidang Penyelenggaraan Haji dan Umrah.
	Perangkat jaringan Internet dan intranet.	Perangkat jaringan yang digunakan sebagai pendukung agar SISKOHAT dapat diakses dan digunakan.
	Printer/ scanner	Alat pendukung untuk mencetak laporan, data jemaah haji ataupun data lainnya.
Software	Antivirus	Antivirus yang digunakan adalah AVAST dan AVG. *Software* pada PC untuk mendeteksi serta mencegah virus yang masuk pada komputer.
	Sistem Operasi PC/*Server*	Digunakan sebagai *software* untuk mendukung sistem ini di bagian sistem operasi.
	JRE (*Java Runtime environment*)	Aplikasi agar data foto *fingerprint* dan foto calon jemaah dapat terlihat pada

		sistem.
	Microsoft Office	Aplikasi pendukung dalam kegiatan proses bisnis pada bidang penyelenggaraan haji dan umrah.
People	Kepala Bidang Penyelenggaraan Haji dan Umrah	*Monitoring* data-data jemaah haji (laporan)
	KASI Sistem Komputerisasi Haji Terpadu	*Monitoring* data jemaah haji dan umrah, dan menginformasikan perubahan-perubahan modul ataupun yang berkaitan dengan sistem, dan informasi jemaah haji.
	KASI Pembinaan Haji dan Umrah	*Monitoring* data Pembimbing haji dan umrah.
	KASI Pendaftaran dan Dokumen Haji	*Monitoring* data dan dokumen haji (verifikasi dokumen)
	KASI Pengelolaan Keuangan Haji	*Monitoring* data keuangaan haji.
	KASI Akomodasi, Transportasi, dan Perlengkapan Haji.	*Monitoring* perlengkapan dan kebutuhan haji.
	Staff Haji dan Operator SISKOHAT	Menjalankan tugas pembatalan dan pendaftaran haji.
Data	Data Jemaah Haji (Reguler dan Khusus)	Biodata dari calon jemaah haji dan umrah yang terdaftar.
	Data Jadwal Keberangkatan	Informasi keberangkatan jemaah haji setiap tahun.
	Data Nomor Porsi	Informasi nomor porsi ataupun estimasi keberangkatan calon jemaah haji.
	Data Pembatalan Jemaah Haji	Informasi biodata jemaah haji yang batal berangkat ataupun tertunda.
	Data Keuangan setelah	Informasi kas haji setelah dilakukan

	audit	audit.
	Data Travel	Informasi terkait data travel agent yang memiliki izin operasi.
	Data Petugas Haji	Informasi terkait data petugas haji yang bertugas atau sebagai pembimbing haji.
	Data KBIH	Data kelompok bimbingan ibadah haji.
Network	Internet	Jaringan yang dimanfaatkan oleh pihak instansi untuk saling bertukar data dan informasi secara meluas, tidak hanya dalam lingkungan instansi namun juga di luar lingkungan instansi. SISKOHAT diakses pada lapisan *end user* (calon jemaah) dapat dilakukan dengan jaringan internet.
	Intranet	Jaringan pribadi atau jaringan komputer yang digunakan oleh instansi untuk berbagi data dan informasi rahasia instansi kepada pegawainya. Dalam hal ini menggunakan jaringan VPN.

4.5.2. Identifikasi Proses Bisnis

Proses bisnis pada Bidang Penyelenggaraan Haji dan Umrah telah didukung oleh Teknlogi Informasi. Sistem yang digunakan adalah Sistem Komputerisasi Haji Terpadu (SISKOHAT). SISKOHAT pada tingkat provinsi merupakan sistem yang berguna untuk memonitor jemaah haji mulai dari pendaftaran, pemberangkatan hingga pemulangan jemaah haji. SISKOHAT yang diterapkan pada tingkat provinsi memiliki fungsi-fungsi seperti pendaftaran haji plus, validasi atau pemeriksaan dokumen haji, pembatalan haji, *monitoring* (jumlah jemaah haji, jumlah pendaftaran calon jemaah haji perhari). SISKOHAT sudah mencakupi seluruh tugas pokok dari kelima seksi dari bidang

penyelenggaraan haji dan umrah. Adapun seksi-seksi tersebut adalah seksi SISKOHAT, seksi Pendaftaran dan Dokumen Haji, seksi Pembinaan Haji dan Umrah, seksi Pengelolaan Keuangan Haji, seksi Akomodasi, Transportasi, dan Perlengkapan Haji. Berikut ini adalah proses bisnis dari SISKOHAT dalam alur proses pendaftaran haji khusus:

1. Calon Jemaah haji membuka rekening tabungan haji pada BPS BPIH.
2. Pengajuan permohonan SPPH ke *travel agent* dengan mengisi formulir SPPH. Adapun syarat-syaratnya adalah:
    a. Surat Keterangan sehat dari dokter
    b. *Fotocopy* KTP dan Kartu Keluarga
    c. *Fotocopy* Akte Kelahiran/ Surat Nikah/ Ijazah
    d. *Fotocopy* buku tabungan
    e. Pas foto terbaru sebanyak 10 lembar dengan latar foto berwarna putih.
3. Pihak *Travel agent* melakukan permohonan SPPH ke kanwil Kemenag Provinsi.
4. Pegawai Kanwil Kemenag Provinsi melakukan pengisian data calon jemaah ke dalam SISKOHAT Gen 2.
5. Dari SISKOHAT Gen 2, akan diperoleh nomor pendaftaran SPPH.
6. *Travel agent* membawa nomor SPPH tersebut ke BPS BPIH dan membayar setoran awal.
7. BPS BPIH melakukan transfer setoran.
8. BPS BPIH memasukkan nomor pendaftaran SPPH.
9. Data pembayaran tersebut secara terintegrasi akan masuk ke dalam basis data SISKOHAT, dan mendapatkan nomor porsi.
10. Setelah transaksi pembayaran berhasil, maka calon jemaah mendapatkan bukti setor BPIH sebanyak 5 lembar.
    a. Lembar pertama (asli) untuk jemaah haji.
    b. Lembar kedua untuk BPS BPIH.
    c. Lembar ketiga untuk PIHK.
    d. Lembar keempat untuk Kanwil Kemenag Provinsi.

e. Lembar kelima untuk direktorat pelayanan Jenderal penyelenggaraan Haji dan Umrah pusat.

11. Calon jemaah melaporkan bukti setor lembar ke 2, 3 dan 4 (kuning, biru, merah).
12. Pegawai melakukan pemeriksaan dan validitas data melalui menu *monitoring* pembayaran.
13. Pegawai memasukkan nomor porsi.
14. Calon jemaah haji telah terdaftar.

Secara keseluruhan, proses bisnis yang dilakukan pegawai dalam menggunakan SISKOHAT Gen 2 yaitu:

1. Pengguna memasukkan url *Virtual Private Number* (VPN) SISKOHAT Gen 2. Kemudian melakukan *log in* dengan *user ID dan Password.*
2. Jika berhasil *log in,* maka halaman utama sistem akan tampil. Jika gagal, maka akan kembali ke halaman *log in*.
3. Memilih menu entry SPPH.
4. Pegawai memasukkan data-data calon jemaah haji.
5. Klik *button* simpan, untuk menyimpan data ke database.
6. Klik *button* cetak untuk mencetak formulir SPPH.
7. Memberikan nomor SPPH kepada calon jemaah untuk selanjutnya melakukan pembayaran.
8. Calon jemaah melaporkan bukti setor dari BPS BPIH.
9. Pegawai mengecek melalui menu *monitoring*.
10. Pegawai mengklik sub menu *monitoring* SPPH Pendaftaran.
11. Pegawai memasukkan nomor porsi calon jemaah.
12. Muncul tampilan data calon jemaah yang sudah terdaftar.
13. Pegawai memilih menu informasi, lalu sub menu informasi *waiting list* jemaah haji.
14. Pegawai memberitahukan estimasi keberangkatan kepada calon jemaah haji.

4.5.3. Pembentukan Tim FMEA

Kegiatan dalam tahapan ini adalah menentukan pihak yang terkait dalam penilaian risiko dengan melalui prosedur pembentukan tim FMEA. Berikut ini prosedur dalam pembentukan tim FMEA:

1. Ukuran tim 1 dan tim 2 masing-masing adalah 3 orang.
2. Anggota tim dipilih berdasarkan kriteria yang telah ditentukan yaitu:
    a. Paling sedikit ada dua teknisi ahli yang termasuk dalam tim FMEA
    b. Orang yang mengetahui tipe-tipe informasi yang berhubungan dengan aset yang terdapat dalam organisasi.
    c. Orang yang mengetahui cara mendapatkan informasi aset tersebut.
    d. Orang yang berkomitmen untuk menyediakan waktu untuk pengukuran risiko.
    e. Orang yang telah berada pada jabatannya minimal satu tahun.
    f. Memiliki otoritas untuk memilih dan memberikan perintah kepada staff untuk mengukur risiko (level manajemen).
3. Ketua tim: Seorang ketua tim harus mengontrol dan mengkoordinasi jalannya proses pengukuran risiko. Adapun hal yang harus di koordinasikan adalah (McDermott et al., 2009):
    a. Mengatur dan memfasilitasi pertemuan termasuk jadwal dan dokumen FMEA yang akan diisi.
    b. Memastikan tim yang bersangkutan hadir.
    c. Memastikan suksesnya pengukuran risiko hingga selesai.

Tim 1 beranggotakan satu orang Kepala Seksi SISKOHAT, satu orang praktisi TI, dan satu orang sebagai koordinator tim. Sedangkan tim 2 beranggotakan satu orang operator, satu orang praktisi TI, dan satu orang sebagai koordinator tim. Praktisi TI pada tim pertama adalah Dr. Okfalisa, S.T., M.Sc. Beliau merupakan Dosen dan sekaligus menjabat sebagai Wakil Dekan III pada Fakultas Sains dan Teknologi UIN SUSKA Riau. Pemilihan praktisi melihat kualifikasi yang dimiliki oleh beliau dalam bidang Teknologi dan Sistem Informasi. Praktisi TI pada tim kedua adalah Eki Saputra, S.Kom., M.Kom. Beliau adalah Dosen pada jurusan sistem informasi, Fakultas Sains dan

Teknologi, UIN SUSKA Riau. Pemilihan praktisi telah sesuai dengan kualifikasi yang telah ditentukan. Beliau juga merupakan dosen pengampu mata kuliah Keamanan Sistem Informasi serta Jaringan Komputer dan Bisnis. Sehingga, kualifikasi Beliau sesuai dengan yang dibutuhkan dalam penelitian ini.

Profil informan yang menjadi narasumber dalam penilaian risiko adalah Bapak Drs. H. Asril selaku Kepala Seksi SISKOHAT. Beliau telah menjabat sebagai KASI SISKOHAT selama 2 tahun dan sebelumnya menjabat sebagai KASI Pembinaan Haji dan Umrah lebih kurang 5 tahun. Kemudian, pada tim kedua adalah Bapak Nik Yusri selaku operator SISKOHAT yang telah bekerja sebagai operator selama 15 tahun.

Tabel 4.18. Tim FMEA

Tim 1	Tim 2
Dr. Okfalisa, S.T.,M.T	Eki Saputra, S.Kom, M.Kom
Nina Fadilah Najwa, S.Kom	Nina Fadilah Najwa, S.Kom
H. Asril (KASI SISKOHAT)	Nik Yusri (Operator SISKOHAT)

4.5.4. Menentukan Metode Penilaian

Pada tahapan ini menyatukan persepsi untuk menggunakan dokumen FMEA *Improvement* dan skala kriteria yang telah dibuat. Dengan penentuan metode penilaian menggunakan metode FMEA memberikan hasil yang konsisten walaupun dilakukan oleh tim yang berbeda. Karena telah berdasarkan prosedur untuk menentukan metode yang disepakati.

A. Desain Dokumen FMEA

Desain dokumen FMEA yang telah dibuat untuk digunakan dan telah di validasi adalah:

Tabel 4.19. Desain Dokumen FMEA *Improvement*

Kode	**Aset Kritis**	**(impact) Mode Potensi Kegagalan**	***Potensi Efek kegagalan***	***SEV***	**(threat) *Potensi penyebab/ mekanisme***	**Sumber ancaman**	***OCC***	***Current Compensanting Controls* (Compensate Vulnerability)**		***RPN***
								Kontrol pencegahan	**Kontrol deteksi**	
<kode aset>	<nama aset>	<dampak akhir jika terjadinya ancaman>	Kategori dampak	1	Ancaman	*<people, process, technology>*	1	Pencegahan	*Monitoring*	1

Keterangan:

1. Kode : Kode risiko sebagai penomoran yang menjadi kode unik masing-masing risiko.
2. Aset Kritis : pengelompokan risiko berdasarkan aset kritis yang telah didefinisikan pada tahapan *brainstorming* potensi kegagalan.
3. Mode Potensi Kegagalan (*Potential failure mode)*: Keadaan akhir dampak terjadinya ancaman (akibat terjadinya ancaman) yang dalam hal ini disebut sebagai risiko.
4. Potensi efek kegagalan (*Potential effect of failure*) :Efek keparahan yang terjadi terhadap pelayanan/operasional, perhatian media, dan regulasi. Kategori potensi efek diselaraskan dengan parameter tingkat keparahan (*severity*).
5. Tingkat Keparahan (*severity*): skala 1 hingga 5 yang terbagi menjadi 3 dampak, yaitu pelayanan/operasional, perhatian media, dan regulasi.
6. Potensi penyebab/mekanisme (*Potential cause/mechanism of failure*): penyebab terjadinya risiko (ancaman).
7. Sumber ancaman (*source of threat*): kategorisasi sumber ancaman yang dibagi menjadi 3 kategori, yaitu: orang (*people*), proses (*process*) dan teknologi *(technology*).
8. Tingkat terjadi (*Occurrence*): skala 1 hingga 5 yang memprediksi tingkat terjadinya risiko.

9. (*Current Compensanting Controls (Compensate Vulnerability*)): kontrol yang dilakukan untuk mengatasi kelemahan organisasi yang terdiri dari kontrol pencegahan (*Preventive Control*) dan kontrol deteksi *(Detective Control*).

B. Skala Kriteria

Penggunaan skala kriteria yang telah divalidasi adalah skala 1-5. Berikut ini adalah skala kriteria yang dimaksudkan:

1. Kriteria skala *severity*

Tingkat keparahan terdiri dari lima skala. Tingkat keparahan dibedakan dengan tiga dampak yaitu tingkat keparahan terhadap pelayanan atau operasiona, tingkat keparahan terhadap perhatian media, tingkat keparahan terhadap finansial & regulasi.

Tabel 4.20. Kriteria skala tingkat keparahan (severity) FMEA *improvement*

Skala	**Level Skala**	**Tingkat keparahan terhadap**		
		Pelayanan/ operasional	**Perhatian media**	**Regulasi**
1	Sangat Kecil	Tidak Berdampak	Tidak berdampak	Tidak Berdampak
2	Kecil	Dampak dapat diabaikan	Potensi menjadi sorotan publik	Percobaan akses ke SISKOHAT.
3	Sedang	Kegiatan operasional ataupun kinerja terhambat.	Pemberitaan negatif pada media massa	Sistem operasional ditembus oleh *hacker/cracker*
4	Besar	Pelayanan terhadap calon jemaah terganggu lebih dari 24 jam.	Ekspos utama (di media massa) lebih dari satu hari	Investigasi oleh pihak berwajib atau *regulatory*
5	Sangat Besar	Ketidaknyamanan yang berarti/ keresahan timbul dari seluruh calon jemaah.	Menjadi perhatian pemerintah / kehilangan kepercayaan publik	Kegagalan sistem menyeluruh / sistem secara total tidak berfungsi.

2. Kriteria Skala *occurrence*

Kriteria skala tingkat terjadi terdiri dari lima kategori. Mulai dari dapat diabaikan, kecil kemungkinan terjadinya risiko, kemungkinan terjadi sedang atau bias terjadinya risiko, kemungkinan besar terjadi dan akan terjadinya risiko dalam berbagai situasi.

Tabel 4.21. Kriteria Skala Tingkat Terjadi (*occurrence*) FMEA *improvement*

Skala	**Level Skala**	**Tingkat Terjadi**
1	Sangat Tidak Mungkin	Dapat diabaikan
2	Mungkin	Kecil kemungkinan terjadi
3	Kadang-kadang	Kemungkinan terjadi sedang / Bisa Terjadi
4	Hampir Pasti	Kemungkinan besar terjadi
5	Pasti Terjadi	Akan terjadi (dalam segala situasi)

3. Level Risiko

Pengkategorian level risiko dilakukan seperti tabel di bawah ini:

Tabel 4.22. Level Risiko FMEA *improvement*

Inherent Risk		***Risk Level***	***Action Plan***
1-5	*Low*	Diterima	-
6-10	*Low to Medium*	Diterima	-
11-15	*Medium*	Diterima	-
16-20	*Medium to High*	Tidak Diterima	Dihilangkan, dikurangi, dipindahkan
21-25	*High*	Tidak Diterima	Dihilangkan, dikurangi, dipindahkan

4.5.5. Pelatihan dan Pemahaman Prosedur

Tahapan pelatihan dilakukan untuk memberikan pengetahuan dan pemahaman FMEA *improvement* kepada tim yang akan mengukur risiko. Kegiatan pelatihan mencakup pemberian materi prosedur digunakan untuk

menjelaskan detail langkah-langkah yang perlu dilakukan dalam menganalisis dan menilai risiko menggunakan metode FMEA*improvement*. Kemudian, dengan adanya pelatihan menyatukan persepsi dan pengetahuan dari anggota tim terhadap risiko TI yang akan dinilai(Carlson, 2014). Keluaran dari pelatihan ini dibataskan pada modul umum tata cara penggunaan dokumen FMEA sebagai persiapan awal sebelum dilakukan penilaian risiko. Adapunmekanisme pelatihanyang dilakukan adalah:

Tabel 4.23. Mekanisme Pelatihan

Pra-Pelatihan	Pelatihan
1. Persiapan modul/materi pelatihan 2. Pemateri 3. Peserta 4. Jadwal pelatihan 5. Peralatan pendukung	Penyampaian materi dan demo pengisian nilai FMEA.

4.5.6. *Brainstorming* Potensi Kegagalan (*failure mode, potential effect, potential cause*)

Brainstorming potensi kegagalan sebelumnya telah dilakukan identifikasi aset kritis. Identifikasi aset kritis dilakukan untuk mengetahui aset teknologi informasi yang dimiliki oleh studi kasus yang akan diteliti. Kemudian, langkah selanjutnya membangun profil ancaman berbasis aset. Selanjutnya, identifikasi kerentanan infrastruktur (Alberts & Dorofee, 2002).

4.5.6.1.Profil Aset Berbasis Ancaman

Sama halnya dengan tahapan yang dilakukan pada siklus *action research* pertama, tahapan-tahapan dalam membangun profil berbasis ancaman adalah sebagai berikut:

A. Profil kebutuhan keamanan

Profil kebutuhan keamanan Teknologi Informasi dibangun berdasarkan aspek keamanan informasi yaitu *Confidentiality, Integrity*, dan *Availability* (Whitman & Mattord, 2012), (Alberts & Dorofee, 2002).

Tabel 4.24. Profil Kebutuhan Keamanan

Aset Kritis	***Confidentiality***	***Integrity***	***Availability***
		Hardware	
Server	Harus dijamin kredibilitas serta kepastian sistem terhadap pengguna yang berhak	Harus dijaga keberadaannya dari orang yang tidak berhak baik secara fisik dan logika	*Server* harus bisa digunakan secara optimal selama 24 jam 7 hari
Komputer/PC	Harus dijamin kerahasiaan *log in* pada komputer yang digunakan	Tidak boleh ada yang bisa *log in* ke sistem kecuali orang yang berhak	Perangkat komputer harus bisa berfungsi selama jam kerja
Perangkat jaringan internet, intranet	Letak perangkat jaringan harus diletakkan diluar jangkauan pihak yang tidak berwenang	Konfigurasi jaringan hanya boleh dilakukan oleh administrator.	Harus dapat menyambungkan berbagai koneksi internet dan data ke *server* dan jaringan luar maupun lokal.
Printer/ scanner	Dipergunakan seoptimal mungkin oleh pihak yang berwenang.	Hanya orang yang berkepentingan saja yang dapat menggunakan perangkat.	Harus dapat berfungsi selama jam kerja.
		Software	
Antivirus	Yang berhak mengganti atau melakukan *upgradesoftware* hanya teknisi atau operator.	Antivirus yang digunakan tidak boleh meyerang data-data penting perusahaan	Antivirus dapat mendeteksi serangan virus kapanpun.
Sistem Operasi PC/*Server*	Tidak boleh diakses oleh pihak yang tidak berwenang	Tidak boleh mengganti sistem operasi tanpa izin.	Sistem operasi harus dapat digunakan selama jam kerja berlangsung.

JRE Microsoft Office	Yang berhak mengganti atau melakukan *upgradesoftware* hanya teknisi atau operator.	Tidak boleh mengganti atau menghapus *software* ini tanpa izin.	Dapat digunakan selama jam kerja berlangsung.
People			
Kepala Bidang Penyelenggaraan Haji dan Umrah KASI Sistem Komputerisasi Haji Terpadu KASI Pembinaan Haji dan Umrah KASI Pendaftaran dan Dokumen Haji KASI Pengelolaan Keuangan Haji KASI Akomodasi, Transportasi, dan Perlengkapan Haji.	Melihat laporan pada sistem sesuai dengan hak akses.	Tidak dapat merubah dan menghapus data calon jemaah haji.	*Monitoring* dapat dilakukan selama jam kerja.
Staff Haji dan Operator SISKOHAT	Pegawai yang akan menggunakan sistem harus mendapatkan pelatihan terlebih dahulu.	Tidak adanya pemalsuan dan kesalahan dalam penginputan data calon jemaah haji.	Harus siap melayani ketersediaan sistem selama 24 jam dan 7 hari.
Data			
Data Jemaah Haji (Reguler dan Khusus) Data Pembatalan Jemaah Haji Data Keuangan	Tidak boleh dilihat oleh orang yang tidak memiliki hak otorisasi karena data tersebut bersifat rahasia.	Tidak bisa memodifikasi data-data yang telah diinputkan. Dan data tidak boleh diambil oleh orang yang	Data dapat diakses ketika dibutuhkan.

setelah audit		tidak berwenang.	
Data Nomor Porsi Data Jadwal Keberangkatan	Hanya bisa dilakukan pengecekan oleh pihak kemenag (operator) pada SISKOHAT Kemenag, dan calon jemaah haji (pemilik nomor porsi) yang diakses pada situs Kemenag.	Hanya fungsi *view*, tidak dapat memodifikasi data.	Data dapat diakses 24 jam 7 hari.
Network			
Internet	Pihak yang *log in* ke sistem harus dilindungi kerahasiaan autentikasinya.	Tidak boleh ada yang bisa *log in* ke sistem kecuali orang yang berhak.	Jaringan tersedia selama 24 jam 7 hari.
Intranet	Sambungan jaringan hanya dapat digunakan di perangkat dan lokasi tertentu.	Perangkat yang tidak disetujui tidak boleh disambungkan ke jaringan.	Jaringan dapat digunakan selama jam kerja.

Sumber: Olahan Peneliti, 2014

B. Ancaman terhadap aset kritis

Ancaman internal merupakan potensi kemungkinan terjadinya serangan yang bersumber dari internal organisasi. Sedangkan ancaman ekternal merupakan potensi kemungkinan terjadinya serangan yang berasal dari eksternal organisasi. Penyusunan ancaman tersebut juga berdasarkan kondisi dari lapangan dan wawancara yang telah dilakukan. Sedangkan untuk mendefinisikan risiko yang bersumber dari kedua hal tersebut, dilakukan penyusunan ancaman internal dan

eksternal dengan melihat kategorisasi ancaman (Whitman & Mattord, 2012). Berikut ini adalah daftar ancaman yang diidentifikasi dari aset kritis:

Tabel 4.25. Ancaman aset kritis

Kategori Aset	**Aset Kritis**	**Ancaman**	
		Internal	**Eksternal**
Hardware	*Server*	- Kebakaran *Server* yang mengalami *overheat* - *Serveroverheat* karena tidak berfungsinya AC pada ruangan - *Server down* karena terlalu banyaknya unit yang mengakses *server* pada waktu bersamaan. - *Server* rusak karena Tidak adanya proses *controlling* dan *maintenance* secara rutin sehingga menyebabkan penurunan kinerja dan kerusakan pada *server*.	- Terjadinya bencana alam seperti banjir, kebakaran, tersambar petir. (*Force of nature*) - *Server* rusak karena terkena reruntuhan bangunan (*server* terletak di lantai bawah)
	Komputer/PC	- Kesalahan dalam konfigurasi komputer sehingga tidak dapat digunakan - Adanya serangan virus pada PC yang menyebabkan PC menjadi rusak - Lisensi *software* yang digunakan sudah	- Terjadinya bencana alam seperti banjir, kebakaran, tersambar petir. (*Force of nature*) - Hilangnya komponen PC karena pencurian. - Pencurian hak akses PC karena adanya pihak yang tidak bertanggungjawab

		melebihi batas waktu	mencuri informasi hak akses PC untuk dapat mengakses PC.
	Perangkat jaringan internet, intranet	- Kerusakan pada infrastruktur jaringan seperti *switch/hub*, *router*, *access point*. - Manipulasi konfigurasi jaringan.	- Terjadinya bencana alam seperti banjir, kebakaran, tersambar petir. (*Force of nature*) - Hilangnya komponen perangkat jaringan karena pencurian. - Kabel jaringan digigit tikus.
	Printer/ scanner	Rusaknya *printer/ scanner* karena *maintenance* dan kontrol yang tidak rutin.	- Terjadinya bencana alam seperti banjir, kebakaran, tersambar petir. (*Force of nature*) - Hilangnya *printer/ scanner* karena pencurian.
Software	Antivirus Sistem Operasi PC/*Server* Java Microsoft Office	- Lisensi *software* yang digunakan sudah melebihi batas waktu - Serangan virus karena Antivirus tidak mampu mendeteksi dan mencegah virus yang masuk	- Terjadinya bencana alam seperti banjir, kebakaran, tersambar petir. (*Force of nature*)
People	Kabid Penyelenggaraan Haji dan Umrah KASI Sistem Komputerisasi Haji Terpadu KASI Pembinaan	- Penyalahgunaan hak akses yang dimiliki. - *Human failure*, yaitu kesalahan dalam penginputan data dan penggunaan perangkat sistem.	- Adanya kerjasama dengan pihak luar untuk melakukan pemalsuan tanda tangan yang tercatat pada sistem - Pelayanan terhadap calon jemaah haji tidak

	Haji dan Umrah KASI Pendaftaran dan Dokumen Haji KASI Pengelolaan Keuangan Haji KASI Akomodasi, Transportasi, dan Perlengkapan Haji. Staff Haji dan Operator SISKOHAT	- SDM kurang kompeten	maksimal.
Data	Data Jemaah Haji (Reguler dan Khusus) Data Jadwal Keberangkatan Data Nomor Porsi Data Pembatalan Jemaah Haji Data Keuangan setelah audit Data Travel Data Petugas Haji Data KBIH	- Kurangnya pengontrolan kapasitas memori *server* dan storage yang telah terpakai - Penyebaran informasi rahasia oleh pegawai. - Pembobolan informasi terhadap sistem dengan melakukan berbagi *password*. - Ketidakcocokan antara data pada sistem dengan data fisik. - Hilangnya data karena *software failure.* - Kurangnya keamanan pada sistem (*firewall*) - Data korup karena jaringan internet yang kurang optimal. - Data tidak dapat diakses (sistem error)	- Pencurian data atau informasi oleh orang yang tidak berwenang. - Terjadinya bencana alam seperti banjir, kebakaran, tersambar petir. (*Force of nature*)

Network	Internet Intranet	- Jaringan LAN tidak cepat - Konektivitas internet yang menurun - Adanya koneksi terputus - Adanya kesalahan pengalamatan IP	- Penyadapan informasi penting melalui jaringan seperti celah masuknya *hacker* dan *Remote Spying*. - Rusaknya kabel jaringan karena digigit tikus, atau pihak eksternal mengubah posisi kabel.

Sumber: Olahan Peneliti, 2018

C. Keamanan yang sudah diterapkan

Berdasarkan hasil wawancara dan observasi lapangan yang telah dilakukan, berikut ini adalah keamanan yang sudah diterapkan pada bidang ini:

1. Pemantauan ruangan melalui CCTV

Penerapan keamanan dilakukan dengan pemasangan perangkat CCTV untuk memantau keadaan ruangan yang terdapat aset kritis teknologi informasi. CCTV dipasang pada sudut-sudut atas ruangan yang dapat melihat pergerakan keluar dan masuknya orang-orang dari ruangan. CCTV bertujuan juga untuk menjaga aset dari pencurian perangkat, ataupun merekam segala kejadian yang terjadi pada ruangan tersebut.

2. Penggunaan sekat atau pembatas ruangan

Dahulunya ruangan SISKOHAT terdiri satu ruangan yang bebas, dan dilantai atas dikhususkan untuk seksi SISKOHAT. Akan tetapi, pengaturan tersebut masih dirasa kurang aman bagi pihak Kementerian Agama Provinsi Riau. Sehingga, kondisi ruangan dirubah dengan memberikan sekat-sekat ruangan untuk menghindari bebasnya tamu yang masuk. Sekat pada lantai dasar dilakukan dengan memberikan partisi bagi ruangan Kepala Bidang Penyelenggaraan Haji dan Umrah, partisi bagi ruangan pegawai internal termasuk ruangan para KASI. Kemudian, di lantai atas terdapat ruangan bagi Seksi Keuangan Haji. Sehingga,

bagi para tamu (calon jemaah) yang ingin mendapatkan informasi akan mendatangi *counter desk operator* yang ditemui saat memasuki ruangan Bidang Penyelenggaraan Haji dan Umrah. Dengan demikian, pengawasan dan kontrol terhadap orang-orang yang tidak berkepentingan dapat dilakukan lebih baik.

3. Pengingat untuk mematikan perangkat TI

Setiap hari pada saat jam kerja habis yaitu sekitar pukul 16.00 WIB, terdapat pengumuman yang diperuntukkan bagi seluruh pegawai. Pengumuman untuk mengingatkan pegawai agar mematikan seluruh perangkat komputer yang digunakan, dan mematikan lampu serta AC. Kemudian, *cleaning service* akan melakukan pengecekan ruangan, membersihkan ruangan, dan mengunci ruangan.

4. Jalur masuk satu pintu

Kementerian Agama menerapkan jalur masuk satu pintu dan keluar satu pintu. Hal ini dimaksudkan agar satpam dapat melakukan pengawasan orang-orang yang masuk ke dalam wilayah kantor Kementerian Agama Provinsi Riau. Sehingga, sebagai tamu harus wajib lapor dan memberitahukan kepentingannya kepada satpam. Selanjutnya, satpam akan memberikan arahan dan petunjuk kepada tamu.

5. Penggunaan jaringanVPN (*Virtual Private Network*)

SISKOHAT hanya dapat diakses menggunakan link VPN (Virtual Private Network) jaringan pribadi (bukan untuk akses umum) yang menggunakan medium nonpribadi (misalnya internet) untuk menghubungkan antar *remote-site* secara aman. Hanya Kepala Bidang, Kepala Seksi dan staff pada bidang penyelenggaraan haji dan umrah saja yang mengetahui alamat VPN tersebut. Dan alamat VPN antara KASI dan Staf juga berbeda, sehingga tingkat keamanan lebih tinggi. VPN dapat diakses oleh orang-orang yang telah memiliki wewenang (*username* dan *password*) untuk dapat masuk ke jaringannya. Setelah berhasil masuk jaringan, maka akan masuk ke halaman *log in* SISKOHAT. Kemudian, SISKOHAT dapat diakses dengan memasukkkan *username* dan *password* yang telah dimiliki. Jika terjadi tiga kali kesalahan dalam *log in*, maka akun akan di

blokir. Sehingga, pengurusannya dilakukan dengan melakukan koordinasi kepada Kemenag Pusat untuk mendapatkan akun kembali ataupun *reset password*.

6. Kondisi lingkungan

Gedung Kanwil Kemenag Riau merupakan kepemilikan pemerintah. Gedung berada di tengah kota Pekanbaru dan terletak pada jalur protokol kota Pekanbaru. Kanwil Kemenag Riau belum pernah mengalami kebakaran, kejatuhan pesawat, banjir, angin topan, gempa bumi, gunung meletus, tsunami, pencurian, huru-hara, fluktuasi tegangan, tertabrak mobil, dan tertimpa pohon. Bidang Penyelenggara haji dan umrah memiliki ruangan yang luas dan struktur bangunan yang kuat dan kokoh. Gedung Bidang Penyelenggaraan Haji dan Umrah ini terdiri dari dua lantai bertingkat dengan tangga. Lantai bawah merupakan operator melayani calon jemaah yang ingin mendapatkan informasi haji, atau mengumpulkan dokumen, serta terdapat ruangan pegawai dan ruangan Kepala Bidang. Sedangkan lantai atas merupakan ruang Seksi Keuangan Haji. *Server* terletak pada gedung yang terpisah, yaitu dibagian Bidang Informasi Masyarakat (Inmas) berada pada lantai dasar.

7. Pembatasan hak akses

Pada Bidang Penyelenggaraan Haji dan Umrah tingkat Provinisi hanya bisa melakukan input data dan *monitoring* data (*view*). Sedangkan menu edit dan hapus dilakukan oleh Kanwil Kemenag RI. Sehingga, jika terjadi kesalahan penginputan data ataupun proses pembatalan calon jemaah haji, dilakukan dengan koordinasi dengan pihak pusat untuk perbaikan data. Hal ini dilakukan sebagai upaya kecermatan dalam penginputan data dan menghindari modifikasi data oleh orang yang tidak berwenang ataupun penyalahgunaan hak akses.

8. Penggantian *password*

Penggantian *password* dilakukan oleh Kanwil Kemenag RI, dan secara rutin penggantian *password* minimal dilakukan 1 kali dalam setahun. Adapun pengeditan akun juga dilakukan dengan meminta persetujuan dan dilakukan oleh Kemenag RI.

D. Kelemahan organisasi

Berdasarkan hasil observasi dan wawancara yang telah dilakukan, maka kelemahan organisasi yang diidentifikasi adalah:

1. *Server* pusat SISKOHAT ada di Jakarta, sehingga apabila *server* di Jakarta mengalami masalah seperti *server down* maka dapat mempengaruhi jaringan pengiriman data di Kanwil Kemenag Provinsi Riau.
2. Tata letak *server* Kanwil Kemenag Provinsi Riau berada pada lantai dasar. Sehingga, terancam mengalami bencana alam seperti keruntuhan bangunan, banjir, dan sebagainya.
3. Masih kurangnya kesadaran instansi terhadap risiko TI. Seperti penjagaan *password* dan *username,* masih terdapat pegawai yang menempelkan *password* dan *username* pada monitor ataupun di atas meja. Sehingga, kerahasiaan akun ataupun hak akses sistem terancam.
4. Dari segi *maintenance hardware* dilakukan secara menyeluruh (Kanwil Kemenag Riau) satu kali dalam setahun yang dilakukan oleh tim dari Kementerian Agama RI. Akan tetapi, hanya *monitoring* dan tidak detail kepada *maintenance* di Bidang Penyelenggaraan Haji dan Umrah. Sedangnya *maintenance hardware* di *monitoring* oleh pihak Kementerian Agama Provinsi Riau setiap satu kali 6 bulan. Belum terdapat dokumentasi *maintenance* yang dilakukan secara prosedural.
5. Tidak ada UPS ataupun Genset. Sehingga tidak adanya penanganan jika lampu mati ataupun tidak cukupnya daya listrik.
6. Belum adanya identifikasi risiko di pada Bidang Penyelenggaraan Haji dan Umrah dalam penggunaan SISKOHAT, sehingga menanganan risiko hanya dilakukan ketika masalah itu terjadi.
7. Belum adanya dokumen yang jelas (user manual) yang detail mengenai penggunaan SISKOHAT.
8. Pelatihan pegawai masih kurang yang dikirimkan sekali dalam setahun. Delegasi tiap provinsi mengutus satu orang untuk mengikuti pelatihan tersebut.

4.5.6.2.Identifikasi Kelemahan Infrastruktur

Berikut ini penjelasan dari identifikasi kelemahan infrastruktur yang ada pada Bidang Penyelenggaraan Haji dan Umrah Kantor Wilayah Kementerian Agama Provinsi Riau.

A. Komponen Utama

Komponen utama menjelaskan mengenai penggunaan infrastruktur dan informasi yang ada pada Bidang Penyelenggaraan Haji dan Umrah sebagai bagian dari proteksi aset TI yang digunakan, yang dijelaskan sebagai berikut :

1. *Server* di dalam Kanwil Kemenag Provinsi Riau terdapat *server* dengan data akan langsung terhubung ke dalam *server* pusat di Jakarta.
2. Jaringan yang digunakan menggunakan VPN untuk mengakses SISKOHAT. Jaringan berupa internet dan intranet.
3. Perangkat PC dan *Printer/ scanner* sebagai perangkat yang digunakan dalam mengakses SISKOHAT, serta perangkat keras yang digunakan mendukung proses bisnis yang ada pada instansi.
4. Antivirus digunakan untuk mendukung maintenance dari setiap *software* dan sistem operasi, yang berfungsi untuk *update* agar meminimalisir virus yang mengancam.
5. *Software* JRE sebagai *software* yang dapat menampilkan data foto *fingerprint* dan foto calon jemaah haji.
6. Sistem Operasi yang digunakan bagi pengguna adalahsistem operasi *Windows 7* ataupun *Windows 10*. Akan tetapi, SISKOHAT lebih *compatible* dengan *Windows 7*.
7. *People* yaitu sumber daya manusia yang mengakses SISKOHAT yaitu para pegawai Bidang Penyelenggaraan Haji dan Umrah.

B. Kerentanan Teknologi Saat Ini

Setelah diperoleh data komponen kunci selanjutnya dilakukan evaluasi terhadap kerentanan komponen kunci tersebut.

Tabel 4.26. Kerentanan Teknologi Saat ini

Komponen Utama	Kerentanan
Server	- *Server* pusat SISKOHAT ada di Jakarta, sehingga apabila *server* di Jakarta mengalami masalah seperti *server down* maka dapat mempengaruhi jaringan pengiriman data di Kanwil Kemenag Provinsi Riau. - Tata letak *server* Kanwil Kemenag Provinsi Riau berada pada lantai dasar. Sehingga, terancam mengalami bencana alam seperti keruntuhan bangunan, banjir, dan sebagainya. - Serangan DDOS yaitu serangan yang biasanya terjadi pada *server* dilakukan melalui jaringan internet sehingga mengacaukan sistem kerja *server*.
Jaringan	Terputusnya koneksi karena jaringan tidak dapat digunakan akibat rusaknya kabel jaringan, serangan *hacker*, ataupun permasalahan *bandwidth.*
PC	Serangan virus yang dapat merusak data-data penting yang ada pada PC.
Antivirus	*Software* tidak dapat melakukan update secara otomatis
JRE	*Software* tidak dapat berfungsi dan menampilkan data foto *fingerprint* dan foto dari calon jemaah haji.
Sistem Operasi	*Software* masih terdapat celah keamanan, seperti penggunaan sistem operasi yang tidak berlisensi. Apabila tidak menggunakan sistem operasi resmi maka apabila terjadi kerusakan dapat menyebabkan sistem operasi tidak berfungsi dan tidak dapat digunakan.
Sistem (SISKOHAT)	Masih terdapatnya celah keamanan. Terdapat kegagalan sistem, kelemahan keamanan.
People	*Social engineering* yang menyebabkan kebocoran data ataupun informasi penting oleh pihak internal kepada pihak eksternal/pihak yang tidak bertanggungjawab.

Sumber: Olahan Peneliti, 2018

4.5.7. Penyusunan *risk register* / Daftar Risiko

Kegiatan dalam tahapan ini adalah memasukkan hasil dari *brainstorming* potensial kegagalan yang diperoleh pada tahapan sebelumnya ke dalam dokumen FMEA yang telah disediakan formatnya. Berikut ini adalah daftar risiko yang telah sesuai dengan desain dokumen FMEA *improvement:*

Tabel 4.27. Susunan daftar risiko FMEA *improvement*

Kode	**Aset Kritis**	**(Impact) Mode Potensi Kegagalan**	***Potensi Efek kegagalan***	***SEV***	**(Threat) *Potensi penyebab/mekanisme***	**Sumber ancaman**	***OCC***	***Current Compensanting Controls* (Compensate Vulnerability)**		***RPN***
								Kontrol pencegahan	**Kontrol deteksi**	
HW01	*Server*	Kebakaran *Server*	Pelayanan/ operasional		*Server* mengalami *overheat*	Teknologi		Pengecekan ruangan *server* setiap hari.	N/A	
HW02		Kebakaran *Server*	Pelayanan/ operasional		Hubungan arus pendek (*power failure*)	Teknologi			Cek infrastruktur TI yang rusak	
HW03		*Serveroverheat*	Pelayanan/ operasional		Tidak berfungsinya AC pada ruangan *server*	Teknologi		Pengecekan ruangan *server* setiap hari.	N/A	
HW04		*Server* down	Pelayanan/ operasional		Terlalu banyaknya unit yang mengakses *server* pada waktu bersamaan ataupun serangan DDOS.	Proses		N/A	Cek infrastruktur TI yang rusak	
HW05		Kerusakan *server*	Pelayanan/ operasional		Tidak adanya proses *controlling* dan *maintenance* secara rutin	Proses		N/A	Cek infrastruktur TI yang rusak	
HW06		Kerusakan *server*	Pelayanan/ operasional		Bencana alam seperti terkena reruntuhan bangunan (*server* terletak di lantai bawah)	Proses		N/A	Cek infrastruktur TI yang rusak	
HW07	Komputer/ PC	Kerusakan Komputer	Pelayanan/ operasional		Adanya serangan virus	Teknologi		Antivirus setiap PC	Cek infrastruktur TI yang rusak	
HW08		Komputer tidak dapat digunakan	Pelayanan/ operasional		Kesalahan dalam konfigurasi komputer	Orang		N/A	Cek infrastruktur TI yang rusak	
HW09		Komputer tidak	Pelayanan/		Lisensi *software* yang digunakan	Teknologi		N/A	Cek infrastruktur TI	

Kode	Aset Kritis	(Impact) Mode Potensi Kegagalan	*Potensi Efek kegagalan*	*SEV*	(Threat) *Potensi penyebab/mekanisme*	Sumber ancaman	*OCC*	*Current Compensanting Controls* (Compensate Vulnerability)		*RPN*
								Kontrol pencegahan	Kontrol deteksi	
		dapat digunakan	operasional		sudah melebihi batas waktu				yang rusak	
HW10		Komputer tidak dapat digunakan	Pelayanan/ operasional		Bencana alam (kebakaran, banjir, petir)	Proses		Mematikan perangkat sebelum pulang	Cek infrastruktur TI yang rusak	
HW11		Perangkat komputer *out of dated*	Pelayanan/ operasional		Usangnya teknologi yang digunakan	Teknologi		N/A	*Monitoring* perangkat sekali dalam setahun	
HW12		Hilangnya komponen PC	Regulasi		Pencurian	Orang		Pembatasan dan pengawasan hak akses ruangan	CCTV	
HW13		Akses informasi PC secara ilegal	Regulasi		Penjagaan hak akses lemah dan atau komputer tidak diberi *password.*	Orang		*Password* masing-masing PC pegawai	CCTV	
HW14	Perangkat jaringan	Kegagalan jaringan	Pelayanan/ operasional		Kerusakan pada infrastruktur jaringan seperti *switch/hub, router, access point*.	Teknologi		N/A	Cek infrastruktur TI yang rusak	
HW15		Kegagalan jaringan	Pelayanan/ operasional		Manipulasi konfigurasi jaringan.	Orang		N/A	Cek infrastruktur TI yang rusak	
HW16		Kerusakan Perangkat Jaringan	Pelayanan/ operasional		Bencana alam (*force of nature*) dan atau hewan	Proses		N/A	Cek infrastruktur TI yang rusak	
HW17		Hilangnya komponen perangkat jaringan	Regulasi		Pencurian	Orang		Pembatasan dan pengawasan hak akses ruangan	CCTV	
HW18	*Printer/ scanner*	Kerusakan *Printer/ scanner*	Pelayanan/ operasional		*Maintenance* dan kontrol yang tidak rutin.	Orang		N/A	Cek infrastruktur TI yang rusak	
HW19		Kerusakan *Printer/ scanner*	Pelayanan/ operasional		Terjadinya bencana alam seperti banjir, kebakaran, tersambar petir. (*Force of nature*)	Proses		Mematikan perangkat sebelum pulang	Cek infrastruktur TI yang rusak	
HW20		Hilangnya *printer/ scanner*	Regulasi		Pencurian	Orang		Pembatasan dan pengawasan hak akses ruangan	CCTV	

Kode	Aset Kritis	(Impact) Mode Potensi Kegagalan	*Potensi Efek kegagalan*	*SEV*	(Threat) *Potensi penyebab/mekanisme*	Sumber ancaman	*OCC*	*Current Compensanting Controls* (Compensate Vulnerability)		*RPN*
								Kontrol pencegahan	Kontrol deteksi	
SW01	Antivirus, Sistem Operasi, JRE, Ms.Office	Kegagalan *Software*	Pelayanan/ operasional		Lisensi *software* yang digunakan sudah melebihi batas waktu	Teknologi		N/A	Cek infrastruktur TI yang rusak	
SW02		Serangan Virus	Pelayanan/ operasional		Antivirus tidak mampu mendeteksi dan mencegah virus yang masuk	Teknologi		N/A	Melakukan update antivirus	
SW03	SISKOHAT	Kegagalan sistem	Pelayanan/ operasional		Sistem masih terdapat celah keamanan	Teknologi		*Maintenance* sistem dilakukan oleh pusat	N/A	
PP01	Kepala dan Staff	Kegagalan Manusia	Perhatian media		Kesalahan dalam penginputan data dan penggunaan perangkat sistem	Orang		Adanya SOP	Pelatihan sekali dalam setahun	
PP02		Kegagalan Manusia	Pelayanan/ operasional		SDM kurang kompeten	Orang		Adanya SOP	Pelatihan sekali dalam setahun	
PP03		Pemalsuan atau penyalahgunaan hak akses	Perhatian media		Kerjasama dengan pihak luar untuk melakukan pemalsuan tanda tangan yang tercatat pada sistem	Orang		Tidak ada hak akses edit/hapus dalam tingkat provinsi.	Penggantian *password* /tahun	
DA01	Data	Penuhnya kapasitas	Pelayanan/ operasional		Kurangnya pengontrolan kapasitas memori *server* dan storage yang telah terpakai	Orang		N/A	Cek infrastruktur TI yang rusak	
DA02		Tersebarnya informasi rahasia	Perhatian media		Penyalahgunaan hak akses	Orang		Adanya aliran data (bertingkat) dalam akses data	N/A	
DA03		Pembobolan data/informasi	Regulasi		Penyebaran informasi rahasia oleh pegawai (berbagi *password*)	Orang		Adanya aliran data (bertingkat) dalam akses data.	N/A	
DA04		Tidak cocoknya data pada sistem dengan data fisik	Perhatian media		Kesalahan input data	Orang		Verifikasi dokumen	Validasi dokumen	

Kode	Aset Kritis	(Impact) Mode Potensi Kegagalan	*Potensi Efek kegagalan*	*SEV*	(Threat) *Potensi penyebab/mekanisme*	Sumber ancaman	*OCC*	*Current Compensanting Controls* (Compensate Vulnerability)		*RPN*
								Kontrol pencegahan	Kontrol deteksi	
DA05		Data Hilang	Regulasi		Kegagalan *software*, jaringan	Teknologi		Data *Backup*	Cek infrastruktur TI yang rusak	
DA06		*Cybercrime* (hacker attack)	Regulasi		Kurangnya keamanan pada sistem (*firewall*)	Teknologi		Penggunaan VPN	N/A	
DA07		Data Korup	Pelayanan/ operasional		Jaringan internet yang kurang optimal.	Teknologi		N/A	Cek infrastruktur TI yang rusak	
NT01	Internet intranet	Koneksi Jaringan putus	Pelayanan/ operasional		Kegagalan jaringan	Teknologi		N/A	Cek infrastruktur TI yang rusak	
NT02		Koneksi Jaringan putus	Pelayanan/ operasional		Rusaknya perangkat jaringan / mati lampu	Teknologi		N/A	Cek infrastruktur TI yang rusak	
NT03		Konektivitas jaringan menurun	Pelayanan/ operasional		Kegagalan jaringan	Teknologi		N/A	Cek infrastruktur TI yang rusak	
NT04		Kesalahan pengalamatan IP	Pelayanan/ operasional		*Human error*	Orang		N/A	Cek infrastruktur TI yang rusak	

4.5.8. Pemberian Nilai Tingkat pada Masing-Masing Parameter

Pemberian nilai masing-masing parameter dilakukan berdasarkan skala kriteria yang telah ditentukan pada tahapan penentuan metode penilaian.Kedua tim mengikuti arahan dari koordinator tim FMEA. Pada sesi pertama, dilakukan pengukuran risiko kepada tim pertama, dan dilanjutkan dengan pengukuran risiko kepada tim kedua. Durasi penilaian dilakukan pembatasan kurang dari 90 menit pada masing-masing tim FMEA sesuai dengan skenario penelitian yang telah dirancang.

4.5.9. Perhitungan RPN

Setelah pemberian nilai pada masing-masing parameter setiap risiko, maka langkah selanjutnya adalah melakukan perhitungan nilai *Risk Priority Number* (RPN). Nilai RPN menjadi acuan dalam melakukan pemrioritasan risiko dengan mengurutkan nilai RPN dari yang paling besar hingga paling kecil. Berdasarkan modifikasi kerangka FMEA yang dilakukan, parameter yang menjadi kunci utama dalam analisis risiko adalah tingkat keparahan (*severity*) dan tingkat terjadi (occurrence). Sesuai dengan hasil penentuan metode penilaian, perhitungan nilai RPN dengan mengalikan nilai tingkat keparahan (*severity*) dan tingkat terjadi (*Occurrence*).

4.5.9.1.Hasil Risiko FMEA *Improvement* Tim 1

Berikut ini adalah hasil dari penilaian risiko yang dilakukan oleh tim FMEA *Improvement* yang pertama.

Tabel 4.28. Hasil Penilaian Risiko FMEA *Improvement* Tim 1

Kode	**Aset Kritis**	**(Impact) Mode Potensi Kegagalan**	***Potensi Efek kegagalan***	***SEV***	**(Threat) *Potensi penyebab/mekanisme***	**Sumber ancaman**	***OCC***	***Current Compensanting Controls* (Compensate Vulnerability)**		***RPN***
								Kontrol pencegahan	**Kontrol deteksi**	
HW01	*Server*	Kebakaran *Server*	Pelayanan/ operasional	4	*Server* mengalami *overheat*	Teknologi	2	Pengecekan ruangan *server* setiap hari.	N/A	8
HW02		Kebakaran *Server*	Pelayanan/ operasional	4	Hubungan arus pendek (*power failure*)	Teknologi	1		Cek infrastruktur TI yang rusak	4
HW03		*Serveroverheat*	Pelayanan/ operasional	2	Tidak berfungsinya AC pada ruangan *server*	Teknologi	2	Pengecekan ruangan *server* setiap hari.	N/A	4
HW04		*Server* down	Pelayanan/ operasional	3	Terlalu banyaknya unit yang mengakses *server* pada waktu bersamaan ataupun serangan DDOS.	Proses	4	N/A	Cek infrastruktur TI yang rusak	12
HW05		Kerusakan *server*	Pelayanan/ operasional	2	Tidak adanya proses *controlling* dan *maintenance* secara rutin	Proses	2	N/A	Cek infrastruktur TI yang rusak	4
HW06		Kerusakan *server*	Pelayanan/ operasional	1	Bencana alam seperti terkena reruntuhan bangunan (*server* terletak di lantai bawah)	Proses	1	N/A	Cek infrastruktur TI yang rusak	1
HW07	Komputer/ PC	Kerusakan Komputer	Pelayanan/ operasional	1	Adanya serangan virus	Teknologi	3	Antivirus setiap PC	Cek infrastruktur TI yang rusak	3
HW08		Komputer tidak dapat digunakan	Pelayanan/ operasional	3	Kesalahan dalam konfigurasi komputer	Orang	2	N/A	Cek infrastruktur TI yang rusak	6
HW09		Komputer tidak dapat digunakan	Pelayanan/ operasional	3	Lisensi *software* yang digunakan sudah melebihi batas waktu	Teknologi	2	N/A	Cek infrastruktur TI yang rusak	6
HW10		Komputer tidak dapat digunakan	Pelayanan/ operasional	2	Bencana alam (kebakaran, banjir, petir)	Proses	1	Mematikan perangkat sebelum pulang	Cek infrastruktur TI yang rusak	2
HW11		Perangkat komputer *out of dated*	Pelayanan/ operasional	1	Usangnya teknologi yang digunakan	Teknologi	1	N/A	*Monitoring* perangkat sekali dalam setahun	1

Kode	Aset Kritis	(Impact) Mode Potensi Kegagalan	*Potensi Efek kegagalan*	*SEV*	(Threat) *Potensi penyebab/mekanisme*	Sumber ancaman	*OCC*	*Current Compensanting Controls* (Compensate Vulnerability)		*RPN*
								Kontrol pencegahan	Kontrol deteksi	
HW12		Hilangnya komponen PC	Regulasi	4	Pencurian	Orang	2	Pembatasan dan pengawasan hak akses ruangan	CCTV	8
HW13		Akses informasi PC secara ilegal	Regulasi	2	Penjagaan hak akses lemah dan atau komputer tidak diberi *password.*	Orang	3	*Password* masing-masing PC pegawai	CCTV	6
HW14	Perangkat jaringan	Kegagalan jaringan	Pelayanan/ operasional	3	Kerusakan pada infrastruktur jaringan seperti *switch/hub, router, access point.*	Teknologi	2	N/A	Cek infrastruktur TI yang rusak	6
HW15		Kegagalan jaringan	Pelayanan/ operasional	3	Manipulasi konfigurasi jaringan.	Orang	2	N/A	Cek infrastruktur TI yang rusak	6
HW16		Kerusakan Perangkat Jaringan	Pelayanan/ operasional	1	Bencana alam (*force of nature*) dan atau hewan	Proses	1	N/A	Cek infrastruktur TI yang rusak	1
HW17		Hilangnya komponen perangkat jaringan	Regulasi	4	Pencurian	Orang	2	Pembatasan dan pengawasan hak akses ruangan	CCTV	8
HW18	*Printer/ scanner*	Kerusakan *Printer/ scanner*	Pelayanan/ operasional	1	*Maintenance* dan kontrol yang tidak rutin.	Orang	1	N/A	Cek infrastruktur TI yang rusak	1
HW19		Kerusakan *Printer/ scanner*	Pelayanan/ operasional	1	Terjadinya bencana alam seperti banjir, kebakaran, tersambar petir. (*Force of nature*)	Proses	1	Mematikan perangkat sebelum pulang	Cek infrastruktur TI yang rusak	1
HW20		Hilangnya *printer/ scanner*	Regulasi	1	Pencurian	Orang	2	Pembatasan dan pengawasan hak akses ruangan	CCTV	2
SW01	Anti virus, Sistem Operasi, JRE, Ms.Office	Kegagalan *Software*	Pelayanan/ operasional	2	Lisensi *software* yang digunakan sudah melebihi batas waktu	Teknologi	3	N/A	Cek infrastruktur TI yang rusak	6
SW02		Serangan Virus	Pelayanan/ operasional	3	Antivirus tidak mampu mendeteksi dan mencegah virus	Teknologi	4	N/A	Melakukan update antivirus	12

Kode	Aset Kritis	(Impact) Mode Potensi Kegagalan	*Potensi Efek kegagalan*	*SEV*	(Threat) *Potensi penyebab/mekanisme*	Sumber ancaman	*OCC*	*Current Compensanting Controls* (Compensate Vulnerability)		*RPN*
								Kontrol pencegahan	Kontrol deteksi	
					yang masuk					
SW03	SISKOHAT	Kegagalan sistem	Pelayanan/ operasional	1	Sistem masih terdapat celah keamanan	Teknologi	1	*Maintenance* sistem dilakukan oleh pusat	N/A	1
PP01	Kepala dan Staff	Kegagalan Manusia	Perhatian media	3	Kesalahan dalam penginputan data dan penggunaan perangkat sistem	Orang	3	Adanya SOP	Pelatihan sekali dalam setahun	9
PP02		Kegagalan Manusia	Pelayanan/ operasional	3	SDM kurang kompeten	Orang	3	Adanya SOP	Pelatihan sekali dalam setahun	9
PP03		Pemalsuan atau penyalahgunaan hak akses	Perhatian Media	5	Kerjasama dengan pihak luar untuk melakukan pemalsuan tanda tangan yang tercatat pada system	Orang	2	Tidak ada hak akses edit/hapus dalam tingkat provinsi.	Penggantian *password* /tahun	10
DA01	Data	Penuhnya kapasitas	Pelayanan/ operasional	2	Kurangnya pengontrolan kapasitas memori *server* dan *storage* yang telah terpakai	Orang	1	N/A	Cek infrastruktur TI yang rusak	2
DA02		Tersebarnya informasi rahasia	Perhatian media	5	Penyalahgunaan hak akses	Orang	2	Adanya aliran data (bertingkat) dalam akses data	N/A	10
DA03		Pembobolan data/informasi	Regulasi	3	Penyebaran informasi rahasia oleh pegawai (berbagi *password*)	Orang	4	Adanya aliran data (bertingkat) dalam akses data.	N/A	12
DA04		Tidak cocoknya data pada sistem dengan data fisik	Perhatian Media	2	Kesalahan input data	Orang	2	Verifikasi dokumen	Validasi dokumen	4
DA05		Data Hilang	Regulasi	1	Kegagalan *software*, jaringan	Teknologi	1	Data *Backup*	Cek infrastruktur TI yang rusak	1
DA06		*Cybercrime* (hacker attack)	Regulasi	1	Kurangnya keamanan pada sistem (*firewall*)	Teknologi	1	Penggunaan VPN	N/A	1
DA07		Data Korup	Pelayanan/ operasional	5	Jaringan internet yang kurang optimal.	Teknologi	4	N/A	Cek infrastruktur TI yang rusak	20

Kode	Aset Kritis	(Impact) Mode Potensi Kegagalan	*Potensi Efek kegagalan*	*SEV*	(Threat) *Potensi penyebab/mekanisme*	Sumber ancaman	*OCC*	*Current Compensanting Controls* (Compensate Vulnerability)		*RPN*
								Kontrol pencegahan	Kontrol deteksi	
NT01	Internet intranet	Koneksi Jaringan putus	Pelayanan/ operasional	4	Kegagalan jaringan	Teknologi	4	N/A	Cek infrastruktur TI yang rusak	16
NT02		Koneksi Jaringan putus	Pelayanan/ operasional	2	Rusaknya perangkat jaringan / mati lampu	Teknologi	1	N/A	Cek infrastruktur TI yang rusak	2
NT03		Konektivitas jaringan menurun	Pelayanan/ operasional	5	Kegagalan jaringan	Teknologi	5	N/A	Cek infrastruktur TI yang rusak	25
NT04		Kesalahan pengalamatan IP	Pelayanan/ operasional	1	*Human error*	Orang	1	N/A	Cek infrastruktur TI yang rusak	1

4.5.9.2.Hasil Risiko FMEA *Improvement* Tim 1

Berikut ini adalah hasil dari penilaian risiko yang dilakukan oleh tim FMEA *Improvement* yang kedua.

Tabel 4.29. Hasil Penilaian Risiko FMEA *Improvement* Tim 2

Kode	**Aset Kritis**	**(Impact) Mode Potensi Kegagalan**	***Potensi Efek kegagalan***	***SEV***	**(Threat) *Potensi penyebab/mekanisme***	**Sumber ancaman**	***OCC***	***Current Compensanting Controls* (Compensate Vulnerability)**		***RPN***
								Kontrol pencegahan	**Kontrol deteksi**	
HW01	*Server*	Kebakaran *Server*	Pelayanan/ operasional	1	*Server* mengalami *overheat*	Teknologi	2	Pengecekan ruangan *server* setiap hari.	N/A	2
HW02		Kebakaran *Server*	Pelayanan/ operasional	4	Hubungan arus pendek (*power failure*)	Teknologi	1		Cek infrastruktur TI yang rusak	4
HW03		*Serveroverheat*	Pelayanan/ operasional	1	Tidak berfungsinya AC pada ruangan *server*	Teknologi	2	Pengecekan ruangan *server* setiap hari.	N/A	2
HW04		*Server* down	Pelayanan/ operasional	4	Terlalu banyaknya unit yang mengakses *server* pada waktu bersamaan ataupun serangan DDOS.	Proses	4	N/A	Cek infrastruktur TI yang rusak	16
HW05		Kerusakan *server*	Pelayanan/ operasional	2	Tidak adanya proses *controlling* dan *maintenance* secara rutin	Proses	1	N/A	Cek infrastruktur TI yang rusak	2
HW06		Kerusakan *server*	Pelayanan/ operasional	1	Bencana alam seperti terkena reruntuhan bangunan (*server* terletak di lantai bawah)	Proses	1	N/A	Cek infrastruktur TI yang rusak	1
HW07	Komputer/ PC	Kerusakan Komputer	Pelayanan/ operasional	2	Adanya serangan virus	Teknologi	2	Antivirus setiap PC	Cek infrastruktur TI yang rusak	4
HW08		Komputer tidak dapat digunakan	Pelayanan/ operasional	3	Kesalahan dalam konfigurasi komputer	Orang	1	N/A	Cek infrastruktur TI yang rusak	3
HW09		Komputer tidak dapat digunakan	Pelayanan/ operasional	3	Lisensi *software* yang digunakan sudah melebihi batas waktu	Teknologi	2	N/A	Cek infrastruktur TI yang rusak	6
HW10		Komputer tidak dapat digunakan	Pelayanan/ operasional	1	Bencana alam (kebakaran, banjir, petir)	Proses	1	Mematikan perangkat sebelum pulang	Cek infrastruktur TI yang rusak	1
HW11		Perangkat komputer *out of dated*	Pelayanan/ operasional	1	Usangnya teknologi yang digunakan	Teknologi	1	N/A	*Monitoring* perangkat sekali dalam setahun	1

Kode	Aset Kritis	(Impact) Mode Potensi Kegagalan	*Potensi Efek kegagalan*	*SEV*	(Threat) *Potensi penyebab/mekanisme*	Sumber ancaman	*OCC*	*Current Compensanting Controls* (Compensate Vulnerability)		*RPN*
								Kontrol pencegahan	Kontrol deteksi	
HW12		Hilangnya komponen PC	Regulasi	4	Pencurian	Orang	2	Pembatasan dan pengawasan hak akses ruangan	CCTV	8
HW13		Akses informasi PC secara ilegal	Regulasi	3	Penjagaan hak akses lemah dan atau komputer tidak diberi *password.*	Orang	3	*Password* masing-masing PC pegawai	CCTV	9
HW14	Perangkat jaringan	Kegagalan jaringan	Pelayanan/ operasional	4	Kerusakan pada infrastruktur jaringan seperti *switch/hub, router, access point.*	Teknologi	2	N/A	Cek infrastruktur TI yang rusak	8
HW15		Kegagalan jaringan	Pelayanan/ operasional	3	Manipulasi konfigurasi jaringan.	Orang	1	N/A	Cek infrastruktur TI yang rusak	3
HW16		Kerusakan Perangkat Jaringan	Pelayanan/ operasional	1	Bencana alam (*force of nature*) dan atau hewan	Proses	1	N/A	Cek infrastruktur TI yang rusak	1
HW17		Hilangnya komponen perangkat jaringan	Regulasi	4	Pencurian	Orang	2	Pembatasan dan pengawasan hak akses ruangan	CCTV	8
HW18	*Printer/ scanner*	Kerusakan *Printer/ scanner*	Pelayanan/ operasional	1	*Maintenance* dan kontrol yang tidak rutin.	Orang	1	N/A	Cek infrastruktur TI yang rusak	1
HW19		Kerusakan *Printer/ scanner*	Pelayanan/ operasional	1	Terjadinya bencana alam seperti banjir, kebakaran, tersambar petir. (*Force of nature*)	Proses	1	Mematikan perangkat sebelum pulang	Cek infrastruktur TI yang rusak	1
HW20		Hilangnya *printer/ scanner*	Regulasi	1	Pencurian	Orang	1	Pembatasan dan pengawasan hak akses ruangan	CCTV	1
SW01	Anti virus, Sistem Operasi, JRE, Ms.Office	Kegagalan *Software*	Pelayanan/ operasional	1	Lisensi *software* yang digunakan sudah melebihi batas waktu	Teknologi	4	N/A	Cek infrastruktur TI yang rusak	4
SW02		Serangan Virus	Pelayanan/ operasional	3	Antivirus tidak mampu mendeteksi dan mencegah virus	Teknologi	5	N/A	Melakukan update antivirus	15

Kode	Aset Kritis	(Impact) Mode Potensi Kegagalan	*Potensi Efek kegagalan*	*SEV*	(Threat) *Potensi penyebab/mekanisme*	Sumber ancaman	*OCC*	*Current Compensanting Controls* (Compensate Vulnerability)		*RPN*
								Kontrol pencegahan	Kontrol deteksi	
					yang masuk					
SW03	SISKOHAT	Kegagalan sistem	Pelayanan/ operasional	1	Sistem masih terdapat celah keamanan	Teknologi	1	*Maintenance* sistem dilakukan oleh pusat	N/A	1
PP01	Kepala dan Staff	Kegagalan Manusia	Perhatian media	3	Kesalahan dalam penginputan data dan penggunaan perangkat sistem	Orang	3	Adanya SOP	Pelatihan sekali dalam setahun	9
PP02		Kegagalan Manusia	Pelayanan/ operasional	2	SDM kurang kompeten	Orang	3	Adanya SOP	Pelatihan sekali dalam setahun	6
PP03		Pemalsuan atau penyalahgunaan hak akses	Perhatian Media	3	Kerjasama dengan pihak luar untuk melakukan pemalsuan tanda tangan yang tercatat pada system	Orang	2	Tidak ada hak akses edit/hapus dalam tingkat provinsi.	Penggantian *password* /tahun	6
DA01	Data	Penuhnya kapasitas	Pelayanan/ operasional	1	Kurangnya pengontrolan kapasitas memori *server* dan *storage* yang telah terpakai	Orang	1	N/A	Cek infrastruktur TI yang rusak	1
DA02		Tersebarnya informasi rahasia	Perhatian media	4	Penyalahgunaan hak akses	Orang	2	Adanya aliran data (bertingkat) dalam akses data	N/A	8
DA03		Pembobolan data/informasi	Regulasi	5	Penyebaran informasi rahasia oleh pegawai (berbagi *password*)	Orang	3	Adanya aliran data (bertingkat) dalam akses data.	N/A	15
DA04		Tidak cocoknya data pada sistem dengan data fisik	Perhatian Media	2	Kesalahan input data	Orang	1	Verifikasi dokumen	Validasi dokumen	2
DA05		Data Hilang	Regulasi	1	Kegagalan *software*, jaringan	Teknologi	1	Data *Backup*	Cek infrastruktur TI yang rusak	1
DA06		*Cybercrime* (hacker attack)	Regulasi	1	Kurangnya keamanan pada sistem (*firewall*)	Teknologi	1	Penggunaan VPN	N/A	1
DA07		Data Korup	Pelayanan/ operasional	4	Jaringan internet yang kurang optimal.	Teknologi	4	N/A	Cek infrastruktur TI yang rusak	16

Kode	Aset Kritis	(Impact) Mode Potensi Kegagalan	*Potensi Efek kegagalan*	*SEV*	(Threat) *Potensi penyebab/mekanisme*	Sumber ancaman	*OCC*	*Current Compensanting Controls* (Compensate Vulnerability)		*RPN*
								Kontrol pencegahan	Kontrol deteksi	
NT01	Internet intranet	Koneksi Jaringan putus	Pelayanan/ operasional	4	Kegagalan jaringan	Teknologi	4	N/A	Cek infrastruktur TI yang rusak	16
NT02		Koneksi Jaringan putus	Pelayanan/ operasional	1	Rusaknya perangkat jaringan / mati lampu	Teknologi	1	N/A	Cek infrastruktur TI yang rusak	1
NT03		Konektivitas jaringan menurun	Pelayanan/ operasional	5	Kegagalan jaringan	Teknologi	5	N/A	Cek infrastruktur TI yang rusak	25
NT04		Kesalahan pengalamatan IP	Pelayanan/ operasional	1	*Human error*	Orang	1	N/A	Cek infrastruktur TI yang rusak	1

4.5.10. Pemrioritasan Risiko

Hasil *Risk Priority Number* (RPN) pada masing-masing Pemrioritasan hasil risiko mengacu pada skala level risiko yang telah ditentukan. Sehingga, hasil yang diperoleh dari kedua tim adalah sebagai berikut.

4.5.10.1. Pemrioritasan Risiko Tim 1

Dari hasil kategorisasi level risiko, satu resiko berada pada level tertinggi dengan kode risiko 'NT03', yaitu risiko konektivitas jaringan menurun karena adanya kegagalan jaringan. Risiko ini tergolong serius dikarenakan sudah sering terjadi hampir setiap harinya dan pegawai sudah merasa tidak nyaman dengan keadaan tersebut. Kemudian, dua risiko yang berada pada tingkatan *medium to high*, tiga risiko berada pada tingakatan *medium*, 13 risiko berada pada tingkatan *low to medium*, dan 18 risiko berada pada tingkatan *low*.

Tabel 4.30. Hasil Pemrioritasan Risiko Tim 1

Kode	**(Impact)** **Mode Potensi Kegagalan**	**(Threat)** ***Potensi penyebab/mekanisme***	***RPN***	***Level***
NT03	Konektivitas jaringan menurun	Kegagalan jaringan	25	*High*
DA07	Data Korup	Jaringan internet yang kurang optimal.	20	*Medium to High*
NT01	Koneksi Jaringan putus	Kegagalan jaringan	16	*Medium to High*
HW04	*Server* down	Terlalu banyaknya unit yang mengakses *server* pada waktu bersamaan ataupun serangan DDOS.	12	*Medium*
SW02	Serangan Virus	Antivirus tidak mampu mendeteksi dan mencegah virus yang masuk	12	*Medium*
DA03	Pembobolan data/informasi	Penyebaran informasi rahasia oleh pegawai (berbagi *password*)	12	*Medium*
PP03	Pemalsuan atau penyalahgunaan hak akses	Kerjasama dengan pihak luar untuk melakukan pemalsuan tanda tangan yang tercatat pada sistem	10	*Low to Medium*
DA02	Tersebarnya informasi rahasia	Penyalahgunaan hak akses	10	*Low to Medium*
PP01	Kegagalan Manusia	Kesalahan dalam penginputan data dan penggunaan perangkat sistem	9	*Low to Medium*
PP02	Kegagalan Manusia	SDM kurang kompeten	9	*Low to Medium*
HW01	Kebakaran *Server*	*Server* mengalami *overheat*	8	*Low to Medium*
HW12	Hilangnya komponen PC	Pencurian	8	*Low to Medium*
HW17	Hilangnya komponen perangkat jaringan	Pencurian	8	*Low to Medium*
HW08	Komputer tidak dapat digunakan	Kesalahan dalam konfigurasi komputer	6	*Low to Medium*

HW09	Komputer tidak dapat digunakan	Lisensi *software* yang digunakan sudah melebihi batas waktu	6	*Low to Medium*
HW13	Akses informasi PC secara ilegal	Penjagaan hak akses lemah dan atau komputer tidak diberi *password.*	6	*Low to Medium*
HW14	Kegagalan jaringan	Kerusakan pada infrastruktur jaringan seperti *switch/hub, router, access point*.	6	*Low to Medium*
HW15	Kegagalan jaringan	Manipulasi konfigurasi jaringan.	6	*Low to Medium*
SW01	Kegagalan *Software*	Lisensi *software* yang digunakan sudah melebihi batas waktu	6	*Low to Medium*
HW02	Kebakaran *Server*	Hubungan arus pendek (*power failure*)	4	*Low*
HW03	*Serveroverheat*	Tidak berfungsinya AC pada ruangan *server*	4	*Low*
HW05	Kerusakan *server*	Tidak adanya proses *controlling* dan *maintenance* secara rutin	4	*Low*
DA04	Tidak cocoknya data pada sistem dengan data fisik	Kesalahan input data	4	*Low*
HW07	Kerusakan Komputer	Adanya serangan virus	3	*Low*
HW10	Komputer tidak dapat digunakan	Bencana alam (kebakaran, banjir, petir)	2	*Low*
HW20	Hilangnya *printer/ scanner*	Pencurian	2	*Low*
DA01	Penuhnya kapasitas	Kurangnya pengontrolan kapasitas memori *server* dan *storage* yang telah terpakai	2	*Low*
NT02	Koneksi Jaringan putus	Rusaknya perangkat jaringan / mati lampu	2	*Low*
HW06	Kerusakan *server*	Bencana alam seperti terkena reruntuhan bangunan (*server* terletak di lantai bawah)	1	*Low*
HW11	Perangkat komputer *out of dated*	Usangnya teknologi yang digunakan	1	*Low*
HW16	Kerusakan Perangkat Jaringan	Bencana alam (*force of nature*) dan atau hewan	1	*Low*
HW18	Kerusakan *Printer/ scanner*	*Maintenance* dan kontrol yang tidak rutin.	1	*Low*
HW19	Kerusakan *Printer/ scanner*	Terjadinya bencana alam seperti banjir, kebakaran, tersambar petir. (*Force of nature*)	1	*Low*
SW03	Kegagalan sistem	Sistem masih terdapat celah keamanan	1	*Low*
DA05	Data Hilang	Kegagalan *software*, jaringan	1	*Low*
DA06	*Cybercrime* (hacker attack)	Kurangnya keamanan pada sistem (*firewall*)	1	*Low*
NT04	Kesalahan pengalamatan IP	*Human error*	1	*Low*

Sumber : Olahan Peneliti, 2018

4.5.10.2. Pemrioritasan Risiko Tim 2

Sama halnya dengan tim pertama, dari hasil kategorisasi level risiko, satu risiko berada pada tingkat tertinggi dengan kode risiko 'NT03', yaitu risiko konektivitas jaringan menurun karena adanya kegagalan jaringan. Kemudian, tiga risiko yang berada pada tingkatan *medium to high*, dua risiko berada pada tingkatan *medium*, 9 risiko berada pada tingkatan *low to medium*, dan 22 risiko berada pada tingkatan *low*.

Tabel 4.31. Hasil Pemrioritasan Risiko Tim 2

Kode	**(Impact) Mode Potensi Kegagalan**	**(Threat)** ***Potensi penyebab/mekanisme***	***RPN***	***Level***
NT03	Konektivitas jaringan menurun	Kegagalan jaringan	25	*High*
HW04	*Server* down	Terlalu banyaknya unit yang mengakses *server* pada waktu bersamaan ataupun serangan DDOS.	16	*Medium to High*
DA07	Data Korup	Jaringan internet yang kurang optimal.	16	*Medium to High*
NT01	Koneksi Jaringan putus	Kegagalan jaringan	16	*Medium to High*
SW02	Serangan Virus	Antivirus tidak mampu mendeteksi dan mencegah virus yang masuk	15	*Medium*
DA03	Pembobolan data/informasi	Penyebaran informasi rahasia oleh pegawai (berbagi *password*)	15	*Medium*
HW13	Akses informasi PC secara ilegal	Penjagaan hak akses lemah dan atau komputer tidak diberi *password.*	9	*Low to Medium*
PP01	Kegagalan Manusia	Kesalahan dalam penginputan data dan penggunaan perangkat sistem	9	*Low to Medium*
HW12	Hilangnya komponen PC	Pencurian	8	*Low to Medium*
HW14	Kegagalan jaringan	Kerusakan pada infrastruktur jaringan seperti *switch/hub, router, access point*.	8	*Low to Medium*
HW17	Hilangnya komponen perangkat jaringan	Pencurian	8	*Low to Medium*
DA02	Tersebarnya informasi rahasia	Penyalahgunaan hak akses	8	*Low to Medium*
HW09	Komputer tidak dapat digunakan	Lisensi *software* yang digunakan sudah melebihi batas waktu	6	*Low to Medium*
PP02	Kegagalan Manusia	SDM kurang kompeten	6	*Low to Medium*
PP03	Pemalsuan atau penyalahgunaan hak akses	Kerjasama dengan pihak luar untuk melakukan pemalsuan tanda tangan yang tercatat pada sistem	6	*Low to Medium*
HW02	Kebakaran *Server*	Hubungan arus pendek (*power failure*)	4	*Low*
HW07	Kerusakan Komputer	Adanya serangan virus	4	*Low*
SW01	Kegagalan *Software*	Lisensi *software* yang digunakan sudah melebihi batas waktu	4	*Low*

HW08	Komputer tidak dapat digunakan	Kesalahan dalam konfigurasi komputer	3	*Low*
HW15	Kegagalan jaringan	Manipulasi konfigurasi jaringan.	3	*Low*
HW01	Kebakaran *Server*	*Server* mengalami *overheat*	2	*Low*
HW03	*Serveroverheat*	Tidak berfungsinya AC pada ruangan *server*	2	*Low*
HW05	Kerusakan *server*	Tidak adanya proses *controlling* dan *maintenance* secara rutin	2	*Low*
DA04	Tidak cocoknya data pada sistem dengan data fisik	Kesalahan input data	2	*Low*
HW06	Kerusakan *server*	Bencana alam seperti terkena reruntuhan bangunan (*server* terletak di lantai bawah)	1	*Low*
HW10	Komputer tidak dapat digunakan	Bencana alam (kebakaran, banjir, petir)	1	*Low*
HW11	Perangkat komputer *out of dated*	Usangnya teknologi yang digunakan	1	*Low*
HW16	Kerusakan Perangkat Jaringan	Bencana alam (*force of nature*) dan atau hewan	1	*Low*
HW18	Kerusakan *Printer/ scanner*	*Maintenance* dan kontrol yang tidak rutin.	1	*Low*
HW19	Kerusakan *Printer/ scanner*	Terjadinya bencana alam seperti banjir, kebakaran, tersambar petir. (*Force of nature*)	1	*Low*
HW20	Hilangnya *printer/ scanner*	Pencurian	1	*Low*
SW03	Kegagalan sistem	Sistem masih terdapat celah keamanan	1	*Low*
DA01	Penuhnya kapasitas	Kurangnya pengontrolan kapasitas memori *server* dan *storage* yang telah terpakai	1	*Low*
DA05	Data Hilang	Kegagalan *software*, jaringan	1	*Low*
DA06	*Cybercrime* (hacker attack)	Kurangnya keamanan pada sistem (*firewall*)	1	*Low*
NT02	Koneksi Jaringan putus	Rusaknya perangkat jaringan / mati lampu	1	*Low*
NT04	Kesalahan pengalamatan IP	*Human error*	1	*Low*

Sumber: Olahan Peneliti, 2018

4.5.11. Rekomendasi Kontrol

Tahapan ini sebagai dokumentasi untuk evaluasi risiko pada keberlanjutan penilaian risiko yang telah menjalankan rekomendasi kontrol. Akan tetapi, penelitian ini membatasi implementasi hingga mendapatkan nilai RPN untuk melihat konsistensi hasil RPN FMEA *improvement* dari kedua tim.

4.6. Pembahasan *Action research*

4.6.1. Profil Instansi dan Objek Penilaian Risiko TI

Sistem Komputerisasi Haji Terpadu merupakan sistem yang digunakan oleh Bidang Penyelenggaraan Haji dan Umrah, Kanwil Kemenag Riau. Bidang ini mempunyai tugas melaksanakan pelayanan dan bimbingan di bidang penyelenggaraan haji dan umrah.Bidang Penyelenggaraan Haji dan Umrah menyelenggarakan menjalankan fungsi penjabaran dan pelaksanaan kebijaksanaan teknis di bidang penyuluhan, bimbingan jemaah dan petugas, perjalanan dan sarana, dan penyiapan bahan pelayanan dan bimbingan di bidang penyelenggaraan haji dan umrah.

Seluruh bagian dari Bidang Penyelenggaraan Haji dan Umrah menggunakan SISKOHAT dalam proses bisnisnya. Adapun bagian-bagian dari Bidang Penyelenggaraan Haji dan Umrah ini adalah sebagai berikut:

1. Seksi Pendaftaran dan Dokumen Haji: Mempunyai tugas melakukan penyiapan bahan pelaksanaan pelayanan, bimbingan teknis, dan pembinaan di bidang pendaftaran dan dokumen haji.
2. Seksi Pembinaan Haji dan Umrah: Mempunyai tugas melakukan pelayanan dan bimbingan bagi jamaah dan petugas haji.
3. Seksi Akomodasi, Transportasi, dan Perlengkapan Haji: Mempunyai tugas melakukan pelayanan di bidang perjalanan haji, perbekalan dan akomodasi haji.
4. Seksi Pengelolaan Keuangan Haji: Mempunyai tugas melakukan pengelolaan keuangan haji.
5. Seksi Sistem Informasi Haji (SISKOHAT): Mempunyai tugas memberikan informasi tentang kegiatan haji, dan mengurusi permasalahan sistem. Bisa disebut sebagai bagian Teknologi Informasi dalam bidang penyelenggaraan haji dan umrah.

SISKOHAT pada Provinsi Riau ini dikembangkan sejak tahun 2010 hingga saat ini yaitu mulai dari SISKOHAT Generasi 1 yang berbasis *desktop* tahun 2010, dan versi *web* yang merupakan SISKOHAT Generasi 2 tahun 2014 . Alasan dibangunnya Sistem Komputerisasi Haji Terpadu (SISKOHAT) adalah sebagai salah satu kebijakan teknis perhajian tahun 1992 dengan penggunaa

komputer dalam usaha meningkatkan pelayanan pengolahan data dan informasi haji, yang merupakan bagian dari alternatif pemecahan permasalahan untuk peningkatan mutu pelayanan ibadah haji kepada masyarakat. Hal ini dikarenakan meningkatnya jemaah haji dari tahun ke tahun yang jumlahnya ribuan sehingga terjadi masalah berupa sulitnya pendataan, kesalahan data, kehilangan data, sulitnya memonitor penyelenggaraan haji serta proses pendaftaran yang rumit dan lama, maka dibentuk suatu sistem komputerisasi haji yang disebut dengan SISKOHAT ((Haji., 2008) dalam (Najwa, 2016)).

SISKOHAT pada tingkat provinsi merupakan sistem yang berguna untuk memonitor jemaah haji mulai dari pendaftaran, pemberangkatan hingga pemulangan jemaah haji. SISKOHAT yang diterapkan pada tingkat provinsi memiliki fungsi-fungsi seperti pendaftaran haji plus, validasi atau pemeriksaan dokumen haji, pembatalan haji, *monitoring* (jumlah jemaah haji, jumlah pendaftaran calon jemaah haji perhari). Beberapa kemudahan dengan adanya SISKOHAT adalah secara *real time* dapat langsung dihitung jumlah setoranBPIH; Pendaftaran haji dapat dilakukan sepanjang tahun *non-stop*; Menyimpan basis data lengkap seluruh jemaah haji secara terstruktur; Kemudahan dan kecepatan layanan informasi tentang posisi dan status jemaah haji kepadapublik sejak masa pendaftaran sampai masa pemberangkatan, operasional di Arab Saudi hingga kepulangan kembali ke daerah asal di tanah air. Selama lebih dari 2 dekade, SISKOHAT telah memperoleh pencapaian yang signifikan. Sistem ini telah tersambung secara *online* dengan 17 Bank penerima setoran BPIH. Sistem inijuga bisa menginput biodata pendaftar calon haji yang tersebar di 12 embarkasi, 33 provinsi serta 3 daerah kerja serta 20 sektor dan satuan tugas Arafah-Mina di Arab Saudi (Agama, 2016).

Penggunaan SISKOHAT dalam proses bisnis Kementerian Agama Provinsi Riau tentunya memiliki risiko TI. Risiko TI adalah risiko yang terkait dengan penggunaan TI secara intensif untuk mendukung dan memperbaiki proses bisnis dan bisnis secara keseluruhan. Risiko TI juga berkaitan dengan ancaman dan bahaya karena pemakaian TI secara intensif yang mungkin menyebabkan kerusakan yang tidak diinginkan atau tidak terduga, kesalahan penggunaan dan kerugian dalam keseluruhan model bisnis dan termasuk lingkungannya(Spremic

& D, 2008). Sehingga, dengan melakukan pengukuran risiko TI pada Bidang Penyelenggaraan Haji dan Umrah dapat memberikan pengetahuan bagi instansi terkait risiko yang ada pada lingkungannya. Belum pernahnya dilakukan pengukuran risiko TI pada Bidang Penyelenggaraan Haji dan Umrah, dan masih dalam tahap perencanaan untuk penerapan SNI/ISO 27001 paling lambat pada tahun 2018 dalam manajemen keamanan informasi SISKOHAT (Agama, 2016).

4.6.2. Hasil Konsistensi FMEA Tradisional

Beberapa penelitian mengkritisi FMEA karena limitasi atau kelemahan dari penggunaan metode ini. Adanya hasil dari analisis risiko dengan menggunakan FMEA terdapat isu konsistensi dan subjektifitas (Estorilio & Posso, 2010), (Barends et al., 2012), (Oldenhof et al., 2011), (Gary Teng et al., 2006). Penelitian ini membuktikan isu konsistensi tersebut pada bidang Teknologi Informasi (TI). FMEA penggunaannya dalam bidang TI berguna untuk mengamankan aset kritis pada organisasi yaitu berupa keamanan informasi (McDermott et al., 2009).

Pada rumusan masalah pertama mengenai konsistensi hasil dari penggunaan FMEA telah dilakukan implementasi kerangka FMEA tradisional. Implementasi kerangka FMEA tradisional pada Bidang Penyelenggaraan Haji dan Umrah dengan menganalisis risiko SISKOHAT. Pengukuran risiko menggunakan metode FMEA dilakukan oleh dua tim yang berbeda untuk melihat konsistensi FMEA. Hal ini sesuai dengan penelitian yang dilakukan oleh Oldenhof et al (2011) menguji konsistensi FMEA dengan pemberian nilai risiko dari dua tim yang berbeda pada satu studi kasus.

Pada *action research* siklus pertama dilakukan untuk menguji konsistensi FMEA. Tahapan awal dengan mengidentifikasi proses bisnis dan risiko berbasis ancaman mengikuti metodologi yang ada pada OCTAVE. Tahapan ini melibatkan peneliti, Kepala Seksi dan pegawai senior dalam membangun profil aset berbasis ancaman. Dari hasil identifikasi risiko, didapatkan 37 daftar risiko yang telah disesuaikan dengan kerangka FMEA Tradisional. Dokumen FMEA dilakukan verifikasi dan validasi kepada kedua praktisi yang masing-masing perwakilan dari

tim 1 dan tim 2. Kemudian, kedua tim melakukan pengukuran risiko berdasarkan dokumen FMEA yang telah disediakan.

Berdasarkan hasil penelitian pada siklus *action research* pertama didapatkan bahwa adanya perbedaan hasil RPN antara kedua tim. Dari jawaban kedua tim, perbedaan jawaban yang paling signifikan secara berurutan terjadi pada parameter tingkat deteksi, kemudian pada tingkat keparahan dan terakhir pada tingkat terjadi. Ketiga parameter tersebut dikalkulasi sesuai dengan rumus RPN (*severity x occurrence x detection*). Pengurutan nilai RPN adalah nilai yang paling tinggi hingga nilai RPN yang paling rendah. Perolehan RPN pada tim pertama adalah 3 risiko berada pada level *very high*, sedangkan pada tim kedua adalah 7 risiko berada pada level *very high*. Akan tetapi, pada urutan tiga teratas hasil peringkatnya adalah sama-sama berada pada level *very high*.

Hasil penelitian ini sesuai dengan penelitian sebelumnya yang memberikan kritisasi isu konsistensi terhadap FMEA Tradisional. Terutama membuktikan dengan menggunakan metodologi yang dikembangkan oleh Odenholf et all (2011). Perbedaan peringkat risiko ini tentunya memberikan perbedaan juga untuk proses mitigasi selanjutnya. Hal ini dikarenakan, seharusnya prioritas risiko membutuhkan biaya yang lebih besar pada risiko peringkat tertinggi, akan tetapi dengan adanya perbedaan peringkat risiko maka organisasi bisa saja melakukan kesalahan dalam pencegahan atau fokus penanganan. Ketika FMEA digunakan secara tepat, maka FMEA dapat mengantisipasi dan mencegah masalah, mengurangi biaya, mempersingkat waktu produksi, dan mencapai keamanan dan produk/jasa yang terpercaya (Carlson, 2014).

Perbandingan berdasarkan parameter perbedaan atau faktor-faktor yang telah dikemukakan pada penelitian (Estorilio & Posso, 2010). Faktor yang menjadi konsentrasi pada penelitian ini adalah dari segi pengetahuan, tim yang mengukur risiko, pelatihan, *failure history*, waktu penyelesaian dan perbedaan jawaban kedua tim. Hasil perbedaan dari faktor yang ditentukan tersebut juga menjadi input bagi siklus *action research* kedua yaitu sintesis kerangka FMEA yang diperbaiki dan implementasi pada studi kasus yang sama.

Urutan jawaban parameter yang paling membedakan secara signifikan adalah jawaban pada kontrol (deteksi) risiko, tingkat keparahan, dan tingkat

terjadi. Perbedaan jawaban ini mengakibatkan nilai RPN berbeda pada kedua tim dan mempengaruhi prioritisasi risiko TI. Fenomena yang terjadi adalah perbedaan yang jauh dalam memberikan nilai pada risiko yang sama. Seperti pemberian nilai tingkat keparahan pada ID Risiko HW02, tim 1 menjawab tingkat keparahan 6, sedangkan tim 2 menjawab tingkat keparahan 1. Demikian juga dengan ID Risiko HW10, tim 1 menjawab tingkat keparahan 7, sedangkan tim 2 menjawab tingkat keparahan 1. Dikarenakan kedudukan tiap parameter adalah sama (linier), sehingga jika dikalikan dengan nilai lainnya akan sangat mempengaruhi besaran nilai RPN yang diperoleh. Sehingga, dengan adanya kesenjangan tersebut, tentunya didasari faktor faktor mengapa informan memilih angka ataupun nilai tersebut.

FMEA tradisional menggunakan pendekatan dengan skala linier untuk menentukan *severity, occurrence* dan *detection* dengan nilai angka. Kriteria skala ini menjadi permasalahan jika pendefinisian yang tidak jelas dan batasan yang meragukan. Penelitian (Paciarotti et al., 2014) melakukan modifikasi atau perbaikan dari segi skala FMEA. Hal ini dilakukan untuk meminimalisir kekurangan dari FMEA. Penelitian tersebut mendefinisikan skala (1,3,9) dalam pemberian nilai S, O, D dengan tingkat (*high, medium, low*). Membatasi ukuran variabel parameter dapat menjadikan FMEA menjadi metode yang lebih cepat, menjadi lebih efektif serta menghasilkan hasil yang kuat.

Pada *action research* pertama ini menggunakan skala 1-10. Dengan kriteria yang banyak tersebut pada implementasinya, informan sulit menentukan dengan cepat dan tepat untuk memberikan nilai masing-masing risiko pada setiap parameter. Pondasi dari FMEA adalah anggota tim dan hasil masukan dari proses FMEA dan perlu adanya estimasi waktu dan pembagian tugas yang jelas (McDermott et al., 2009).

Kesalahan pendefinisian risiko bergantung pada pengalaman anggota tim dalam menganalisis kegagalan dan familiarnya sistem bagi anggota serta bias kognitif yang diketahui. Dengan demikian, sangat adanya kemungkinan kesalahan manusia. Situasi ini sering terjadi bila sedikit data mengenai kejadian dan efek kegagalan diketahui, sehingga memerlukan subjektivitas(Banghart, 2014). Dari hasil yang tidak konsisten disebabkan oleh subjektivitas ini sehingga perlu adanya

strategi untuk mengatasi subjektifitas tim FMEA dalam melakukan penilaian risiko.

Konsistensi hasil FMEA dapat ditingkatkan dengan membangun keahlian dari beberapa fasilitator yang dapat membantu tim analis untuk menggunakan FMEA supaya lebih efektif dan konsisten dengan mendefinisikan mode kegagalan dan tingkat keparahan, kemungkinan dan indeks yang terdeteksi. Kemudian, dengan pengalaman fasilitator akan membuktikan nilai ketika mengevaluasi dampak dari aksi perbaikan yang telah dilakukan. Strategi kedua yang mungkin dilakukan adalah selalu adanya anggota teknisi ahli dalam sebuah tim, hal ini berdampak pada pemberian nilai. Paling sedikit ada dua teknisi ahli yang termasuk dalam tim FMEA untuk menyeimbangkan perbedaan individu yang signifikan dalam keputusan risiko yang krusial (Oldenhof et al., 2011).

Dapat disimpulkan bahwa terbukti FMEA Tradisional berdasarkan hasil *action research* siklus pertama tidak konsisten. Hal ini didasarkan pada perbedaan nilai RPN dan perangkingan dari hasil pengukuran risiko pada kedua tim yang berbeda pada satu kasus yang sama. Sehingga, selanjutnya ke tahap implementasi *action research* untuk perbaikan kerangka FMEA agar hasil yang didapatkan menjadi konsisten.

4.6.3. Hasil Konsistensi FMEA yang Disintesis (FMEA *Improvement*)

FMEA yang disintesis (FMEA *Improvement*) merupakan kerangka perbaikan dari limitasi yang ditemukan pada FMEA tradisional. Kritikal analisis terkait FMEA tradisional menghasilkan titik kelemahan FMEA berdasarkan tahapan FMEA tradisional dan dokumen FMEA. Titik kelemahan tersebut didapatkan dari hasil analisis kesenjangan yang dilakukan pada siklus *action research* pertama dan studi literatur yang telah mengkritisi kelemahan FMEA.

Titik kelemahan yang ditemukan antara lain adalah sulitnya mencari akar permasalahan dari penyebab potensial, sulitnya mengevaluasi faktor risiko secara tepat, pendefinisian dan batasan tidak jelas/meragukan, sifat non-linier dari skala peringkat individu 1-10, subjektifitas/*human error*, bias, memakan waktu yang lama dalam penilaian risiko, tingkat kepentingan parameter sama, RPN identik/duplikat, dan formulasi rumus RPN. Kelemahan-kelemahan tersebut dapat

diminimalisir dengan mendiagnosis penyebab kelemahan tersebut. Berdasarkan penelitian terdahulu, dapat diketahui bahwa titik rawan yang terjadinya isu konsistensi FMEA adalah saat melakukan penilaian risiko (evaluasi risiko). Penilaian risiko dilakukan berdasarkan dokumen FMEA berupa daftar risiko dan skala kriteria sebagai panduan dalam memberikan nilai setiap parameter. Dokumen FMEA tersebut perlu diperhatikan sehingga dalam penilaian risiko yang dilakukan oleh tim FMEA dapat diminimalisir isu konsistensinya.

Dari hasil identifikasi kelemahan dan diagnosa penyebab, diberikan rekomendasi solusi yang disintesis menjadi suatu metodologi kerangka FMEA yang ditingkatkan untuk meminimalisir kelemahan FMEA tradisional. Adapun tahapan FMEA yang disintesis (FMEA *Improvement*) tersebut terdiri dari 4 tahapan utama yaitu penentuan kebutuhan penilaian risiko, identifikasi risiko, analisa dan evaluasi risiko, dan rekomendasi kontrol. Metodologi kerangka FMEA yang disintesis telah divalidasi oleh pakar dan diuji pada studi kasus. Pengujian dilakukan pada studi kasus yang sama dan tim yang sama seperti siklus *action research* pertama, yaitu Bidang Penyelenggaraan Haji dan Umrah, Kantor Wilayah Kementerian Agama Provinsi Riau.

Berdasarkan penilaian risiko yang dilakukan oleh kedua tim, berikut ini adalah detil perbedaan dari hasil kedua tim yang menggunakan kerangka FMEA yang disintesis (FMEA *Improvement*):

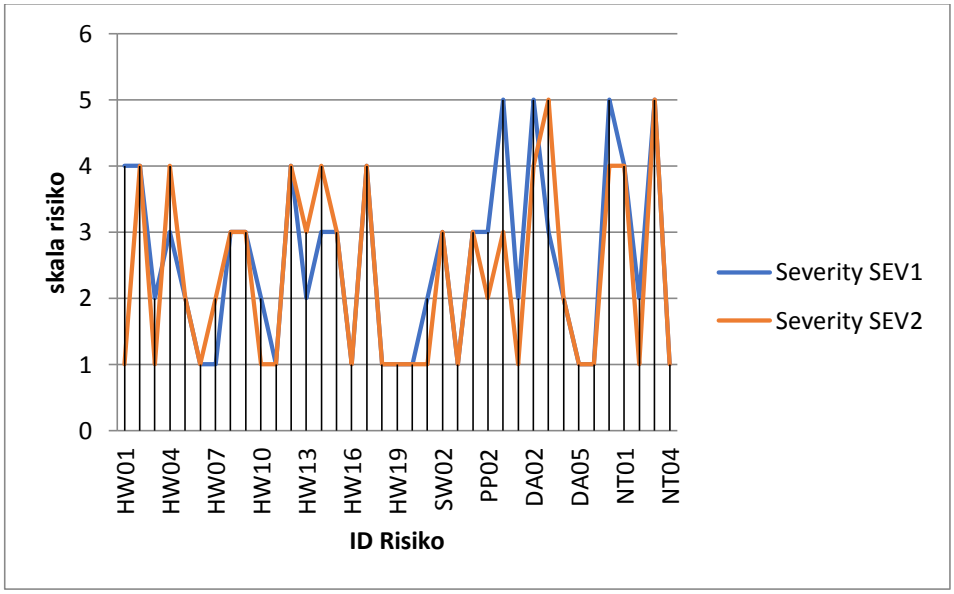
1. Perbedaan waktu penyelesaian

Tim pertama menyelesaikan penilaian risiko dalam kurun waktu 40 menit, sedangkan tim kedua menyelesaikan penilaian risiko dalam kurun waktu 30 menit. Kedua tim telah sesuai dengan ekspektasi penelitian ini yaitu tercapainya penilaian risiko yang kurang dari 90 menit. Hal ini berarti kelemahan terkait lamanya proses penilaian risiko telah diminimalisir. Waktu penilaian yang berkurang juga berdampak pada terminimalisirnya isu subjektifitas dan bias, karena jika waktu penentuan lebih lama membuat tim penilai akan berfikir mengikuti emosi dan perasaan(McDermott et al., 2009), (Estorilio & Posso, 2010).

2. Perbedaan jawaban setiap risiko pada parameter (*severity* dan *occurrence*)

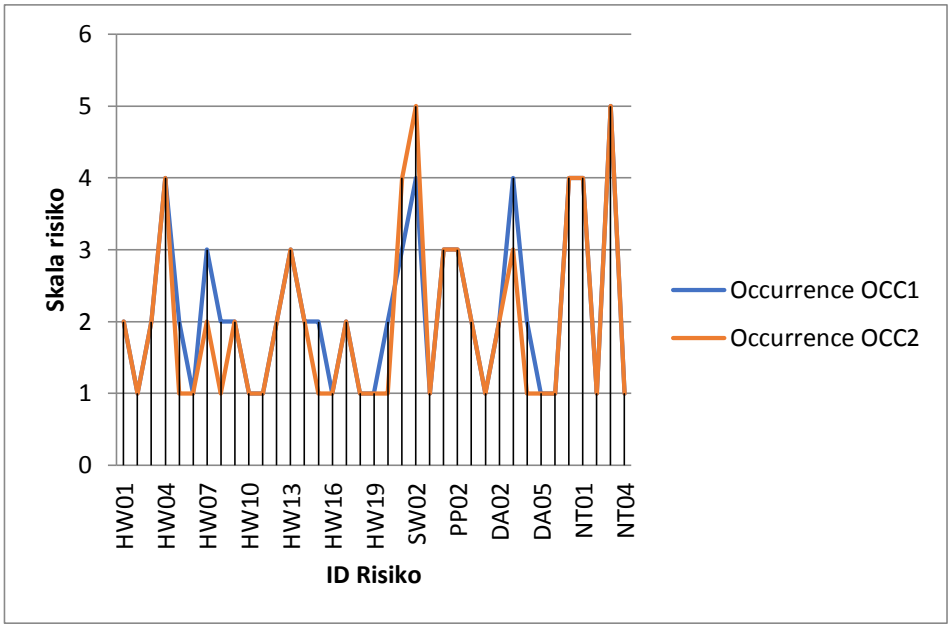
Pada tim pertama dan kedua menghasilkan nilai RPN yang dapat terbilang konsisten. Tim pertama dan kedua sama-sama memperoleh nilai RPN tertinggi 25 pada risiko dengan kode risiko 'NT03', yaitu risiko konektivitas jaringan menurun karena adanya kegagalan jaringan. Risiko ini tergolong serius dikarenakan sudah sering terjadi hampir setiap harinya dan pegawai sudah merasa tidak nyaman dengan keadaan tersebut.

Pada tim pertama, dua risiko yang berada pada tingkatan *medium to high*, tiga risiko berada pada tingakatan *medium*, 13 risiko berada pada tingkatan *low to medium*, dan 18 risiko berada pada tingkatan *low*. Sedangkan pada tim kedua, tiga risiko yang berada pada tingkatan *medium to high*, dua risiko berada pada tingkatan *medium*, 9 risiko berada pada tingkatan *low to medium*, dan 22 risiko berada pada tingkatan *low*. Perbedaan pemberian nilai pada masing-masing parameter (*severity*, *occurrence*) dapat dilihat pada grafik di bawah ini:



Gambar 4.6. Perbandingan Jawaban *Severity* (Tim 2)

Pada grafik di atas dapat dilihat bahwa kemiripan penilaian lebih banyak dibandingan kesenjangan pada penilaian risiko tingkat keparahan siklus pertama. Adapun perbedaan jawaban *occurrence* antara tim 1 dan tim 2 juga memiliki banyak kemiripan.



Gambar 4.7. Perbandingan Jawaban *Occurrence* (Tim 2)

Pada tim pertama dan kedua telah diberikan pelatihan terkait prosedur FMEA *improvement*. Pelatihan ini sangat membantu dalam menyamakan persepsi antar anggota tim terkait prosedur FMEA *improvement* dan mengenai risiko yang ada pada studi kasus. Kemudian, dengan skala tingkat keparahan telah disesuaikan dengan risiko yang ada pada organisasi. Tingkat keparahan dibagi menjadi ke dalam tiga kategori risiko dampak yaitu terhadap risiko layanan/operasional, risiko perhatian media, dan risiko regulasi.Dengan adanya pengkategorian tersebut memangkas halaman dokumen FMEA menjadi lebih efisien. Hal ini karena di kolom tabel potensi efek kegagalan telah disesuaikan dengan kategorisasi risiko. Modifikasi dokumen FMEA dan skala kriteria ini mampu meminimalisir kelemahan FMEA yaitu kesulitan mencari akar masalah dan kesulitan mengevaluasi risiko secara tepat.

Kelemahan terkait tingkat kepentingan parameter telah terbukti dapat diminimalisir dengan menghilangkan variabel deteksi. Hal ini sesuai dengan justifikasi dilakukan, bahwa kunci utama dalam analisis risiko adalah parameter tingkat keparahan dan tingkat terjadi. Dengan pengurangan variabel deteksi juga mengurangi waktu penilaian risiko. Dapat disimpulkan bahwa FMEA

improvement ini dapat meminimalisir kelemahan-kelemahan FMEA yang telah diidentifikasi.

4.6.4. Perbandingan Hasil *Action research*

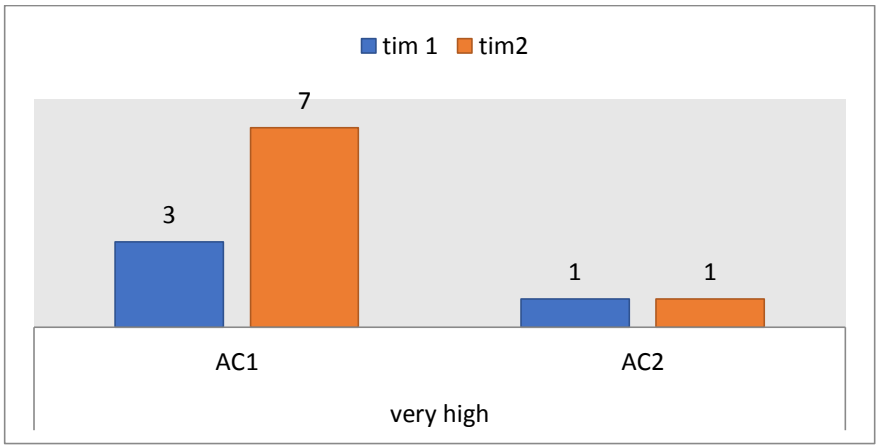
Penelitian ini terdiri dari dua siklus *action research.* Siklus *action research* pertama adalah pengujian konsistensi FMEA tradisional. Pengujian dilakukan pada dua tim yang berbeda dan pada satu studi kasus yang sama. Konsistensi yang dimaksudkan adalah adanya perbedaan hasil *Risk Priority Number* (RPN) diantara kedua tim. Perbedaaan tersebut menjadi masukan dalam menganalisis kesenjangan kedua tim dalam menggunakan FMEA tradisonal. Analisis kritisasi FMEA mengidentifikasi titik-titik kelemahan FMEA tradisional. Dari kelemahan yang telah diidentifikasi didiagnosis penyebab kelemahannya dan diberikan rekomendasi solusi berdasarkan hasil penelitian terdahului. Rekomendasi solusi disintesis menjadi sebuah metodologi perbaikan kerangka FMEA tradisional yang diberi nama FMEA *improvement.*

Pada siklus *action research* pertama terbukti bahwa FMEA tradisional menghasilkan nilai yang tidak konsisten. Dari jawaban kedua tim, perbedaan jawaban yang paling signifikan secara berurutan terjadi pada parameter tingkat deteksi, kemudian pada tingkat keparahan dan terakhir pada tingkat terjadi. Ketiga parameter tersebut dikalkulasi sesuai dengan rumus RPN (*severity x occurrence x detection*). Pengurutan nilai RPN adalah nilai yang paling tinggi hingga nilai RPN yang paling rendah. Perolehan RPN pada tim pertama adalah 3 risiko berada pada level *very high*, sedangkan pada tim kedua adalah 7 risiko berada pada level *very high*. Akan tetapi, pada urutan tiga teratas hasil peringkatnya adalah sama-sama berada pada level *very high*.

Pada siklus *action research* kedua kelemahan yang diidentifikasi dapat diminimalisir berdasarkan hasil yang didapatkan. Pada tim pertama dan kedua menghasilkan nilai RPN yang dapat terbilang konsisten. Tim pertama dan kedua sama-sama memperoleh nilai RPN tertinggi 25 pada risiko dengan kode risiko ‘NT03’, yaitu risiko konektivitas jaringan menurun karena adanya kegagalan jaringan. Risiko ini tergolong serius dikarenakan sudah sering terjadi hampir setiap harinya dan pegawai sudah merasa tidak nyaman dengan keadaan tersebut.

Pada tim pertama, dua risiko yang berada pada tingkatan *medium to high*, tiga risiko berada pada tingakatan *medium*, 13 risiko berada pada tingkatan *low to medium*, dan 18 risiko berada pada tingkatan *low*. Sedangkan pada tim kedua, tiga risiko yang berada pada tingkatan *medium to high*, dua risiko berada pada tingkatan *medium*, 9 risiko berada pada tingkatan *low to medium*, dan 22 risiko berada pada tingkatan *low*. Lebih jelasnya, perbandingan hasil kesenjangan pada kedua *action research* dapat digambarkan pada grafik di bawah ini.

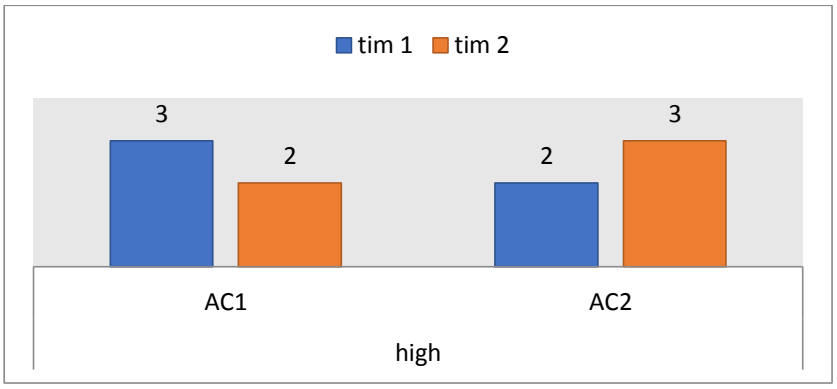
1. Kesenjangan RPN *Very High* Tim 1 dan Tim 2 pada *action research* 1 dan 2.



Gambar 4.8. Perbandingan RPN *Action Research* (AC) *Very High*

Pada gambar 4.8 dapat dilihat bahwa pada siklus *action research* pertama kesenjangan hasil RPN pada level *very high* adalah 4 risiko. Pada tim pertama, risiko yang palig tinggi berjumlah 3, sedangkan pada tim kedua berjumlah 7. Berbeda dengan siklus *action research* kedua, tim pertama dan kedua memiliki jumlah hasil RPN *very high* yang sama. Hal ini berarti sensitivitas perubahan pada level ini adalah tinggi. Perubahan kerangka FMEA yang disintesis (FMEA *Improvement*) terbukti berdampak tinggi terhadap level risiko yang tinggi, dan memberikan hasil yang konsisten.

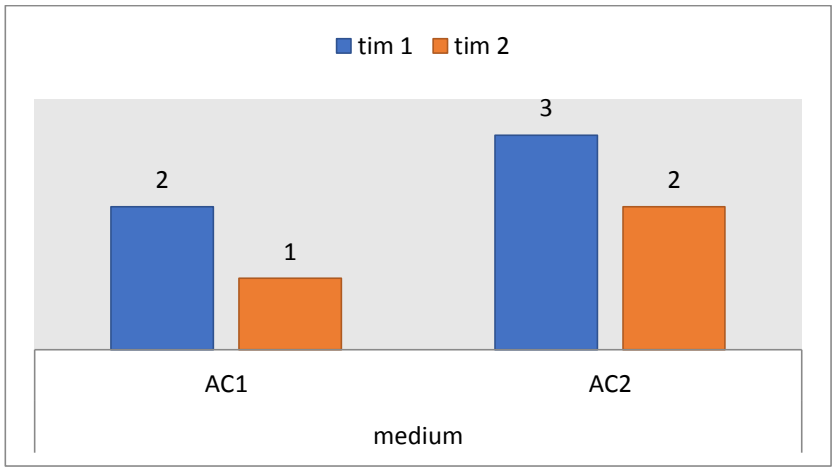
2. Kesenjangan RPN *High* Tim 1 dan Tim 2 pada *action research* 1 dan 2.



Gambar 4. 9. Perbandingan RPN *Action research* (AC) *High*

Perbandingan RPN pada *level high* antara siklus *action research* pertama dan siklus *action research* kedua tidak adanya kesenjangan yang signifikan. Kedua *action research* tersebut memiliki nilai kesenjangan 1 antara tim 1 dan tim 2.

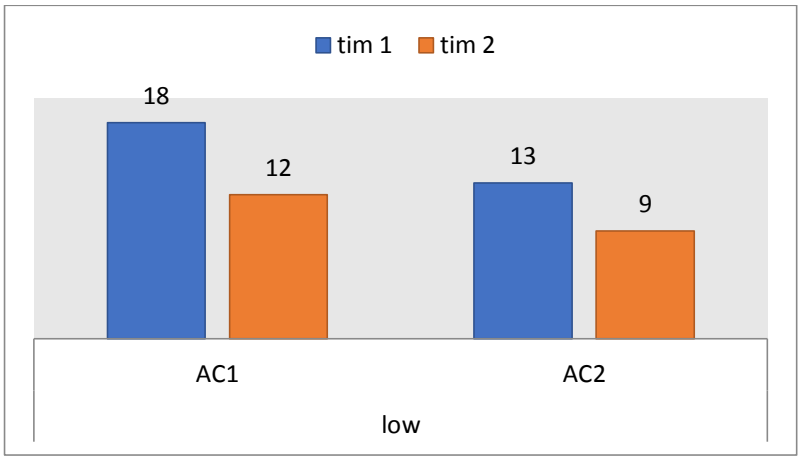
3. Kesenjangan RPN *Medium* Tim 1 dan Tim 2 pada *action research* 1 dan 2.



Gambar 4.10. Perbandingan RPN *Action research* (AC) *Medium*

Perbandingan RPN pada *level medium* antara siklus *action research* pertama dan siklus *action research* kedua tidak adanya kesenjangan yang signifikan. Kedua *action research* tersebut memiliki nilai kesenjangan 1 antara tim 1 dan tim 2.

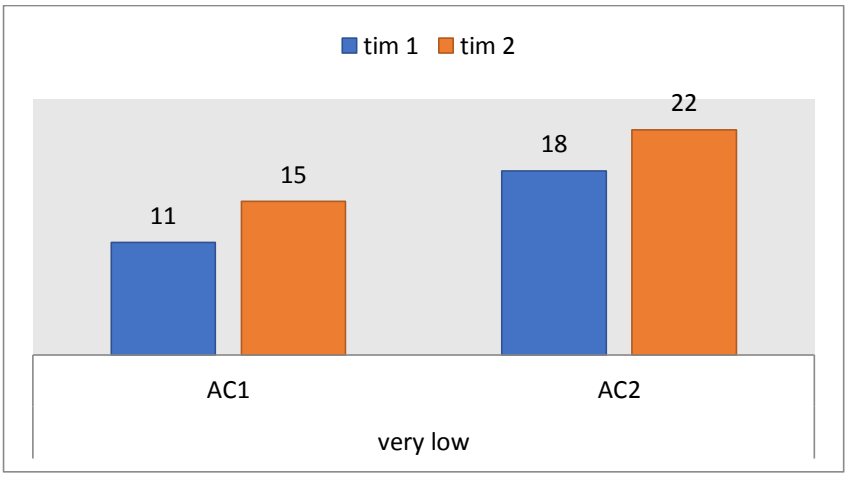
4. Kesenjangan RPN *Low* Tim 1 dan Tim 2 pada *action research* 1 dan 2.



Gambar 4.11. Perbandingan RPN *Action research* (AC) *Low*

Perbandingan RPN pada *level low* antara siklus *action research* pertama dan siklus *action research* kedua memiliki perbedaan nilai pada masing-masing tim. Tim pertama kesenjangannya adalah 6, sedangkan tim kedua kesenjangannya adalah 4. Sehingga, sensitivitas pada siklus *action research* kedua tinggi. Hal ini dikarenakan, pada siklus kedua kesenjangannya semakin kecil.

5. Kesenjangan RPN *Very Low* Tim 1 dan Tim 2 pada *action research* 1 dan 2.



Gambar 4.12. Perbandingan RPN *Action research* (AC) *very low*

Perbandingan RPN pada *level medium* antara siklus *action research* pertama dan siklus *action research* kedua tidak adanya kesenjangan yang signifikan. Kedua *action research* tersebut memiliki nilai kesenjangan 1 antara tim 1 dan tim 2.

Secara lebih detail, perbedaan konsistensi FMEA dapat di lihat pada korelasi antar kedua tim pada masing-masing *action research* (Lampiran G). Analisis korelasi merupakan alat uji yang digunakan untuk mengetahui seberapa besar konsistensi RPN yang dihasilkan oleh kedua siklus. Hal ini berkaitan dengan urutan prioritisasi risiko yang pada setiap level risiko (*very high, high, medium, low,* dan *very low*). Hasil uji analisis korelasi dengan menggunakan SPPS Inc 2017, berdasarkan nilai *pearson correlation.* Penggambaran kesenjangan nilai RPN pada tim 1 dan tim 2 dijelaskan dengan grafik *scatter plot.* Adapun rentang dari kategori tingkat korelasi adalah(de Vaus, 2002):

Tabel 4.32. Interpretasi Koefisien Korelasi

Koefisien	**Level**
0.00	Tidak ada korelasi
0.01-0.09	*Trivial* korelasi (sangat kecil)
0.10-0.29	Kecil
0.30-0.49	Sedang
0.50-0.69	Besar
0.70-0.89	Sangat Besar
0.90+	Hampir sempurna

1. Korelasi Siklus *Action Research* 1

Pada siklus *action research* 1 memiliki perbedaan RPN yang signifikan antara tim 1 dan tim 2. Pada setiap level risiko juga memiliki urutan yang berbeda. Sehingga, berikut ini adalah hasil uji korelasi untuk melihat konsistensi berdasarkan id_risiko pada RPN yang didapatkan.

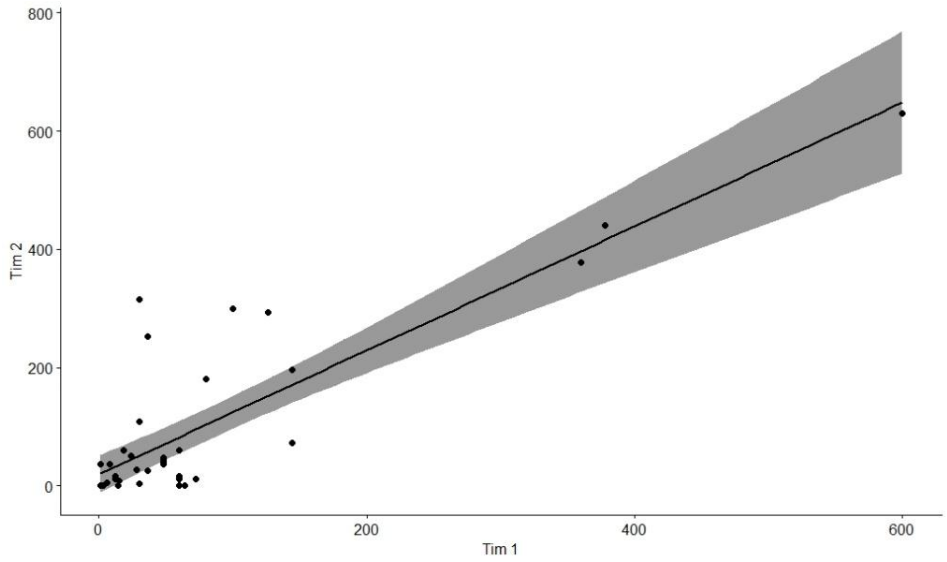
Tabel 4.33. Korelasi *Action Research* 1

		RPN1	RPN2
RPN1	Pearson Correlation	1	.848**
	Sig. (2-tailed)		.000
	N	37	37
RPN2	Pearson Correlation	.848**	1
	Sig. (2-tailed)	.000	
	N	37	37

**. Correlation is significant at the 0.01 level (2-tailed).

Sumber: Olahan Peneliti,2018

Pada tabel di atas, diketahui bahwa nilai korelasi *pearson* pada siklus *action research* 1 adalah 0.848. Hal ini berarti hubungan korelasi tergolong ke dalam korelasi sangat besar. Secara lebih jelas, dapat dilihat kesenjangan yang signifikan dengan gambar *scatter plot* di bawah ini:



Gambar 4.13. Kesenjangan RPN Tim 1 dan Tim 2 (*Action research* 1)

Pada *scatter plot* tersebut, terlihat bahwa kesenjangan yang cukup jauh pada bidang abu-abu yang menggambarkan persebaran RPN Tim 1 dan Tim 2 berdasarkan nilai RPN.

2. Korelasi Siklus *Action Research* 2

Pada siklus *action research* 2 kesenjangan RPN yang dihasilkan pada setiap level risiko telah dapat diminimalisir. Akan tetapi, pada setiap level risiko juga memiliki urutan yang berbeda. Sehingga, berikut ini adalah hasil uji korelasi untuk melihat konsistensi berdasarkan id_risiko pada RPN yang didapatkan.

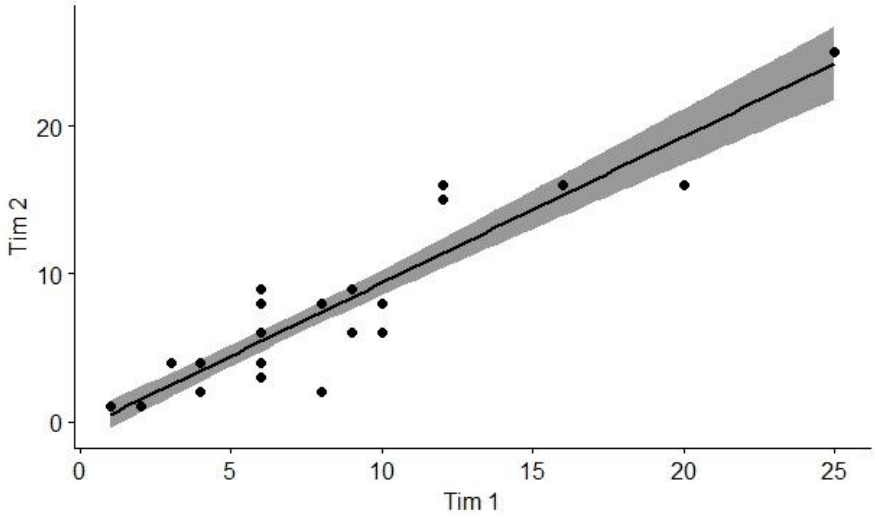
Tabel 4.34. Korelasi *Action Research* 2

		RPN1	RPN2
RPN1	Pearson Correlation	1	.937**
	Sig. (2-tailed)		.000
	N	37	37
RPN2	Pearson Correlation	.937**	1
	Sig. (2-tailed)	.000	
	N	37	37

**. Correlation is significant at the 0.01 level (2-tailed).

Sumber: Olahan Peneliti,2018

Pada tabel di atas, diketahui bahwa nilai korelasi *pearson* pada siklus *action research* 2 adalah 0.937. Hal ini berarti nilai korelasi mendekati 1 yang tergolong ke dalam korelasi hampir sempurna. Secara lebih jelas, dapat dilihat kesenjangan yang signifikan dengan gambar *scatter plot* di bawah ini:



Gambar 4.14. Kesenjangan *Action Research* 2

Pada *scatter plot* tersebut, terlihat bahwa kesenjangan yang tidak cukup jauh pada bidang abu-abu yang menggambarkan persebaran RPN Tim 1 dan Tim 2 berdasarkan nilai RPN.

Sensitivitas tim pada siklus *action research* sangat tinggi terutama pada tingkatan risiko yang tergolong ke dalam *very high.* Dengan modifikasi yang dilakukan pada siklus *action research* kedua dianggap mampu meminimalisir kesenjangan antara tim 1 dan tim 2. Fokus perhatian pada tingkat RPN adalah pada tingkat *very high.* Hal ini dikarenakan, risiko yang berada pada tingkatan *very high* adalah risiko yang memiliki tingkat urgensitas paling tinggi untuk dimitigasi, dihilangkan ataupun di cegah.

Berdasarkan uji korelasi yang dilakukan, konsistensi siklus *action research* 2 bernilai 0.937 yang tergolong dalam korelasi hampir pasti. Sedangkan konsistensi siklus *action research* 1 bernilai 0.848 yang tergolong ke dalam korelasi sangat besar. Dari kedua nilai tersebut dapat terlihat bahwa konsistensi hasil FMEA *Improvement* terbukti lebih konsisten daripada FMEA Tradisional.

Dari segi waktu penyelesaian, pada *action research* pertama tidak adanya estimasi waktu dalam penilaian risiko. Pada *action research* kedua diberikan estimasi waktu untuk meminimalisir isu subjektivitas dan bias dalam penilaian risiko. Estimasi waktu dalam penilaian risiko dilakukan selama kurang dari 90 menit. Tim pertama menyelesaikan penilaian selama 40 menit, sedangkan tim kedua menyelesaikan penilaian selama 30 menit. Dari segi pengetahuan dan pemahaman prosedur, *action research* pertama dan kedua sama-sama diberikan petunjuk tata cara penilaian. Akan tetapi, pada *action research* kedua lebih tersusun dan tahapan pelatihan tersebut dimasukkan ke dalam kerangka FMEA *improvement.*

Tabel 4.35.Hasil Refleksi Penerapan Skenario *Action research*

Skenario *Action Plan*: *Action research 1* dan *Action research 2*		
Tujuan Skenario *Action Plan*: Melakukan pengujian inkonsistensi FMEA tradisional, perbaikan kerangka FMEA, implementasi FMEA *improvement*.		
Dampak yang Diharapkan *(Expected Outcome)*	**Hasil Refleksi 1** *(Reflection Result of Action research 1)*	**Hasil Refleksi 2** *(Reflection Result of Action research 2)*
Kesenjangan RPN yang didapatkan semakin kecil (konsisten)	Terbukti bahwa FMEA tradisional menghasilkan nilai RPN yang tidak konsisten. Menghasilkan analisis kesenjangan yang menjadi masukan untuk siklus selanjutnya.	Terbukti hasil lebih konsisten, sehingga dapat disimpulkan kelemahan FMEA dapat terminimalisir dengan menerapkan kerangka perbaikan FMEA *Improvement*. Perbaikan dilakukan dengan memperbaiki tahapan FMEA. Perbaikan dibuat dengan mensintesis kerangka FMEA dengan rekomendasi solusi. Tahapan yang diformulasikan terdiri dari 4 tahapan utama. Tahapan tersebut adalah penentuan kebutuhan penilaian risiko (identifikasi konteks, identifikasi proses bisnis, pembentukan tim, menentukan metode penilaian, pelatihan), identifikasi risiko (*brainstorming* potensi kegagalan, penyusunan daftar risiko), analisa dan evaluasi risiko (pemberian nilai parameter, perhitungan RPN, pemrioritasan risiko), dan rekomendasi kontrol. Kerangka FMEA yang disintesis telah divalidasi oleh pakar dan diuji pada studi kasus. Dalam masing-masing tahapan tersebut dilakukan intervensi seperti adanya estimasi waktu dalam penilaian risiko yaitu kurang dari 90 menit, serta modifikasi desain dokumen FMEA dengan mengkategorikan dampak risiko menjadi tiga yaitu risiko terhadap operasional/pelayanan, perhatian media dan

		regulasi. Adanya penambahan variabel sumber ancaman yang terdiri dari tiga kategori yaitu orang, teknologi dan proses. Kemudian, skala kriteria yang digunakan dengan rentang 1-5. Pada skala kriteria tingkat keparahan, menggunakan parameter yang jelas berdasarkan jenis kategori dampak risiko. Kemudian, dalam mencari RPN, yang diperhitungkan adalah nilai tingkat keparahan dan nilai tingkat terjadi. Adapun tingkat deteksi tidak dimasukkan dalam penilaian risiko melainkan didefinisikan pada dokumen FMEA nya saja.

(Halaman ini sengaja dikosongkan)

BAB 5
KESIMPULAN DAN SARAN

5.1. Kesimpulan

FMEA yang disintesis (FMEA *Improvement*) merupakan kerangka perbaikan dari limitasi yang ditemukan pada FMEA tradisional. Kritikal analisis terkait FMEA tradisional menghasilkan titik kelemahan FMEA. Kemudian, diagnosa penyebab kelemahan diidentifikasi dan memberikan perbaikan kerangka FMEA. FMEA yang telah disintesis diimplementasikan kembali pada studi kasus untuk melihat konsistensi hasil perbaikan kerangka yang dilakukan. Berdasarkan hasil penelitian yang diperoleh, maka dapat disimpulkan bahwa:

1. FMEA Tradisional berdasarkan hasil *action research* siklus pertama terbukti tidak konsisten. Hal ini dikarenakan hasil RPN tim pertama terdapat 3 risiko pada tingkatan *very high* sedangkan tim kedua terdapat 7 risiko pada tingkatan *very high.*
2. Titik kelemahan yang ditemukan antara lain adalah sulitnya mencari akar permasalahan dari penyebab potensial, sulitnya mengevaluasi faktor risiko secara tepat, pendefinisian dan batasan tidak jelas/meragukan, sifat non-linier dari skala peringkat individu 1-10, subjektifitas/*human error*, bias, memakan waktu yang lama dalam penilaian risiko, tingkat kepentingan parameter sama, RPN identik/duplikat, dan formulasi rumus RPN.
3. Diagnosa penyebab titik kelemahan yang diidentifikasi antara lain adalah pendefinisian sumber ancaman yang kurang tepat, variasi skenario risiko, tidak adanya prosedur pembuatan skala kriteria, penggunaan skala 1-10, belum adanya panduan pembentukan tim, pengalaman dan pengetahuan, tidak adanya batas waktu dalam penilaian, dan tidak adanya bobot nilai atau variabel yang menjadi kunci utama variabel dalam analisis risiko.
4. Tahapan FMEA yang disintesis (FMEA *Improvement*) tersebut terdiri dari 4 tahapan utama yaitu penentuan kebutuhan penilaian risiko (identifikasi konteks, identifikasi proses bisnis, pembentukan tim, menentukan metode penilaian, pelatihan), identifikasi risiko (*brainstorming* potensi kegagalan,

penyusunan daftar risiko), analisa dan evaluasi risiko (pemberian nilai parameter, perhitungan RPN, pemrioritasan risiko), dan rekomendasi kontrol. Kerangka FMEA yang disintesis telah divalidasi oleh pakar dan diuji pada studi kasus.

5. Pada siklus *action research* 2 terbukti bahwa hasil pengukuran risiko dengan FMEA *improvement* lebih konsisten. Hasil RPN yang didapatkan oleh kedua tim adalah sama. Berdasarkan uji korelasi yang dilakukan, konsistensi siklus *action research* 2 bernilai 0.937 yang tergolong dalam korelasi hampir pasti. Sedangkan konsistensi siklus *action research* 1 bernilai 0.848 yang tergolong ke dalam korelasi sangat besar. Dari kedua nilai tersebut dapat terlihat bahwa konsistensi hasil FMEA *Improvement* terbukti lebih konsisten daripada FMEA Tradisional. Dapat disimpulkan kelemahan FMEA dapat terminimalisir dengan menerapkan kerangka perbaikan FMEA *Improvement*.

5.2. Saran

Limitasi dari penelitian ini adalah adanya isu memori karena kedua implementasi *action research* dilakukan pada bidang studi kasus yang sama. Penelitian selanjutnya diharapkan dapat menguji coba perbandingan kerangka FMEA tradisional dan FMEA *improvement* pada studi kasus yang sama dan bidang yang berbeda atau studi kasus yang berbeda. Kemudian, merumuskan faktor kesuksesan implementasi kerangka FMEA agar meningkatkan keakuratan hasil yang diperoleh. Lalu, mencoba kerangka FMEA *improvement* pada studi kasus lainnya (uji konsistensi) dan menggunakan tim yang terdiri dari berbagai disiplin dan bidang (*Cross-functional team activity*) untuk mendapatkan berbagai opini yang berbeda.

DAFTAR PUSTAKA

Agama, K. (2016). Pelayanan Terpadu Satu Pintu & e-Government Saatnya Lebih Melayani. *Media Informasi Kementerian Agama*.

Ahmed, A., Kayis, B., & Amornsawadwatana, S. (2008). A review of techniques for risk management in projects. *Benchmarking: An International Journal*, *14*(1), 22–36. https://doi.org/10.1108/14635770710730919

Alberts, C., & Dorofee, A. (2002). *Managing Information Security Risks : The OCTAVE Approach*. Addison Wesley.

Alexander, K. (1992). Facilities Risk Management. *Facilities*, *10*(4), 14–18. https://doi.org/10.1108/EUM0000000002185

Bandyopadhyay, K., Mykytyn, P. P., & Mykytyn, K. (2011). A framework for integrated risk management in information technology. *Management Decision*, *37*(5), 437–445.

Banghart, M. (2014). Utilizing Confidence Bounds in Failure Mode Effects Analysis (FMEA) Hazard Risk Assessment.

Barends, D. M., Oldenhof, M. T., Vredenbregt, M. J., & Nauta, M. J. (2012). Risk analysis of analytical validations by probabilistic modification of FMEA. *Journal of Pharmaceutical and Biomedical Analysis*, *64–65*, 82–86. https://doi.org/10.1016/j.jpba.2012.02.009

Batbayar, K., Takács, M., & Kozlovszky, M. (2016). Medical device software risk assessment using FMEA and fuzzy linguistic approach : case study. *International Sysmposium on Applied Computational Intelligence and Informatics, 12-14 May 2016. Rimisoara, Romania.*, 197–202.

Cameron, I., Mannan, S., Németh, E., Park, S., Pasman, H., Rogers, W., & Seligmann, B. (2017). Process hazard analysis, hazard identification and scenario definition: Are the conventional tools sufficient, or should and can we do much better? *Process Safety and Environmental Protection*, *110*, 53–70. https://doi.org/10.1016/j.psep.2017.01.025

Carlson, C. S. (2014). Understanding and Applying the Fundamentals of FMEAs. *2014 Annual Reliability and Maintainability Symposium (RAMS)*, 12.

Chai, K. C., Jong, C. H., Tay, K. M., & Lim, C. P. (2016). A Perceptual Computing-based Method to Prioritize Failure Modes in Failure Mode and Effect Analysis and Its Application to Edible Bird Nest Farming. *Applied Soft Computing Journal*. https://doi.org/10.1016/j.asoc.2016.08.043

Chang, D. (2009). Applying DEA to enhance assessment capability of FMEA. *International Journal of Quality & Reliability Management*, *26*(6), 629–643. https://doi.org/10.1108/02656710910966165

Chemweno, P., Pintelon, L., Van Horenbeek, A., & Muchiri, P. (2015). Development of a risk assessment selection methodology for asset maintenance decision making: An analytic network process (ANP) approach. *International Journal of Production Economics*, *170*, 663–676. https://doi.org/10.1016/j.ijpe.2015.03.017

Chen, F. (2015). *An Investigation and Evaluation of Risk Assessment Methods in Information systems*. Chalmers University of Technology, Sweden.

Claxton, K., & Campbell-Allen, N. M. (2017). Failure modes effects analysis

(FMEA) for review of a diagnostic genetic laboratory process. *International Journal of Quality & Reliability Management*, *34*(2), 265–277. https://doi.org/10.1108/IJQRM-05-2015-0073

Creswell, J. W. (2015). *Penelitian Kualitatif & Desain Riset: Memilih di antara Lima Pendekatan*. (S. Z. Qudsy, Ed.) (Edisi Indo). Yogyakarta: Pustaka Pelajar.

de Aguiar, D. C., Salomon, V. A. P., & Mello, C. H. P. (2015). An ISO 9001 based approach for the implementation of process FMEA in the Brazilian automotive industry. *International Journal of Quality & Reliability Management*, *32*(6), 589–602. https://doi.org/10.1108/IJQRM-09-2013-0150

de Vaus, D. . (2002). *Survey In Social Research Fifth Edition* (V). Australia: Allen & Unwin.

Desy, I., Cahyo, B., Hanim, H., Astuti, M., Informasi, J. S., Informasi, F. T., … Sukolilo, I. T. S. (2014). PENILAIAN RISIKO KEAMANAN INFORMASI MENGGUNAKAN METODE FAILURE MODE AND EFFECTS ANALYSIS DI DIVISI TI PT . BANK XYZ SURABAYA. *Seminar Nasional Sistem Informasi Indonesia*, (September).

Emblemsvag, J. (2010). The Augmented Subjective Risk Management Process. *Management Decision*, *48*(2), 248–1747. https://doi.org/10.1108/00251741011022608

Estorilio, C., & Posso, R. K. (2010). The reduction of irregularities in the use of "process FMEA." *International Journal of Quality & Reliability Management*, *27*(6), 721–733. https://doi.org/10.1108/02656711011054579

Firesmith, D. G. (2003). Common Concepts Underlying Safety, Security, and Survivability Engineering, (December). https://doi.org/CMU/SEI-2003-TN-033

Gary Teng, S., Ho, S. M., Shumar, D., & Liu, P. C. (2006). Implementing FMEA in a collaborative supply chain environment. *International Journal of Quality & Reliability Management*, *23*(2), 179–196. https://doi.org/10.1108/02656710610640943

Haji., D. A. D. J. B. M. I. dan U. (2008). *Era Baru Perhajian Melalui Sistem Komputerisasi Haji Terpadu (SISKOHAT)*. Jakarta.

Jacob, P. (2015). Failure analysis and reliability on system level. *Microelectronics Reliability*, *55*(9–10), 2154–2158. https://doi.org/10.1016/j.microrel.2015.06.022

Jain, K. (2017). use of Failure Mode Effect Analysis (FMEA) to Improve Medication Management Process. *International Journal of Health Care Quality Assurance*, *30*(2).

Janneti, A. J. (2012). *A representation: Incorporating a needs assessment and gap analysis into the educational design*. Pitman,NJ : Author.

Kakvan, M., Mohyeddin, M. A., & Gharaee, H. (2014). Risk evaluation of IT service providers using FMEA model in combination with Multi-Criteria Decision-Making Models and ITIL framework. *2014 7th International Symposium on Telecommunications, IST 2014*, 873–878. https://doi.org/10.1109/ISTEL.2014.7000826

Lai, L. K. H., & Chin, K. S. (2014). Development of a Failure Mode and Effects Analysis Based Risk Assessment Tool for Information Security. *Industrial*

Engineering and Management Systems, *13*(1), 87–100. https://doi.org/10.7232/iems.2014.13.1.087

Lipol, L. S., & Haq, J. (2011). Risk analysis method : FMEA / FMECA in the organizations. *International Journal of Basic & Applied Sciences*, *11*(5), 5–74. Retrieved from https://pdfs.semanticscholar.org/c933/f98700fa61900d6f42a86df98c268740c490.pdf

Liu, H. (2015). Improving risk evaluation in FMEA with a hybrid multiple criteria decision making method. *International Journal of Quality & Reliability Management*, *32*(7), 763–782. https://doi.org/10.1108/IJQRM-10-2013-0169

Liu, H., Liu, L., & Liu, N. (2013). Expert Systems with Applications Risk evaluation approaches in failure mode and effects analysis : A literature review. *Expert Systems With Applications*, *40*(2), 828–838. https://doi.org/10.1016/j.eswa.2012.08.010

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding. *MIS Quarterly*, *16*(2), 173. https://doi.org/10.2307/249574

Lolli, F., Gamberini, R., Rimini, B., Pulga, F., Lolli, F., Gamberini, R., & Rimini, B. (2016). A revised FMEA with application to a blow moulding process. *International Journal of Quality & Reliability Management*, *33*(7), 900–919. https://doi.org/10.1108/IJQRM-10-2013-0171

Mason-Blakley, F., & Habibi, R. (2014). Prospective Hazard Analysis for Information System. *Healthcare Informatics (ICHI), 2014 IEEE International Conference on*, 256–265. https://doi.org/10.1109/ICHI.2014.43

McDermott, R. E., Mikulak, R. J., & Beauregard, M. R. (2009). *The Basic of FMEA*. *CRC Press* (2nd ed.). New York: Taylor & Francis Group.

Murphy, M., Heaney, G., & Perera, S. (2011). A methodology for evaluating construction innovation constraints through project stakeholder competencies and FMEA. *Construction Innovation*, *11*(4), 416–440. https://doi.org/10.1108/14714171111175891

Najwa, N. F. (2016). *Analisis Penerimaan Sistem Komputerisasi Haji Terpadu Menggunakan Metode TAM*.

Oldenhof, M. T., van Leeuwen, J. F., Nauta, M. J., de Kaste, D., Odekerken-Rombouts, Y. M. C. F., Vredenbregt, M. J., … Barends, D. M. (2011). Consistency of FMEA used in the validation of analytical procedures. *Journal of Pharmaceutical and Biomedical Analysis*, *54*(3), 592–595. https://doi.org/10.1016/j.jpba.2010.09.024

Paciarotti, C., Mazzuto, G., & D'Ettorre, D. (2014). A revised FMEA application to the quality control management. *International Journal of Quality & Reliability Management*, *31*(7), 788–810. https://doi.org/10.1108/IJQRM-02-2013-0028

Raspotnig, C., & Opdahl, A. (2013). Comparing risk identification techniques for safety and security requirements. *Journal of Systems and Software*, *86*(4), 1124–1151. https://doi.org/10.1016/j.jss.2012.12.002

Rose, S., Spinks, N., & Canhoto, A. I. (2015). *Management Research: Applying the Principles*.

Sankar, R. N., & Prabhu, B. S. (2001). Modified approach for prioritization of

failures in a system failure mode and effects analysis. *International Journal of Quality & Reliability Management*, *18*(3), 324–336. https://doi.org/10.1108/02656710110383737

Sawhney, R., Subburaman, K., Sonntag, C., Rao Venkateswara Rao, P., & Capizzi, C. (2010). A modified FMEA approach to enhance reliability of lean systems. *International Journal of Quality & Reliability Management*, *27*(7), 832–855. https://doi.org/10.1108/02656711011062417

Security, I. 27001. (2008). *An illustration of the application of Failure Modes and Effects Analysis (FMEA) techniques to the analysis of information security risks*. United States of America.

Sellappan, N., Nagarajan, D., & Palanikumar, K. (2015). Evaluation of risk priority number (RPN) in design failure modes and effects analysis (DFMEA) using factor analysis. *International Journal of Applied Engineering Research*, *10*(14), 34194–34198.

Shahin, A. (2004). Integration of FMEA and the Kano model. *International Journal of Quality & Reliability Management*, *21*(7), 731–746. https://doi.org/10.1108/02656710410549082

Sharma, R. K., & Sharma, P. (2010). System failure behavior and maintenance decision making using, RCA, FMEA and FM. *Journal of Quality in Maintenance Engineering*, *16*(1), 64–88. https://doi.org/10.1108/13552511011030336

Sidorova, Evangelopoulos, Valacich, & Ramakrishnan. (2008). Uncovering the Intellectual Core of the Information Systems Discipline. *MIS Quarterly*, *32*(3), 467. https://doi.org/10.2307/25148852

Simister, T. (2000). Risk Management: The Need to Set Standards. *Balance Sheet*, *8*(4), 2–4.

Software, S. P. L. M. (2016). How to conduct a failure modes and effects analysis. *A White Paper Issued by: Siemens PLM Software*. Retrieved from www.siemens.com/polarion

Spremic, M., & D, P. (2008). Emerging issues in IT Governance : implementing the corporate IT risks management model. *Wseas Transactions On Systems*, *7*(3), 219–228.

Stamatis, D. H. (2003). *Failure Mode and Effect Analysis: FMEA from Theory to Execution* (illustrate). Milwaukee, Wisconsin: ASQ Quality Press.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology. *Nist Special Publication 800*, *30*(July).

Sutrisno, A., Gunawan, I., Vanany, I., & Khorshidhi, H. A. (2016). A maintenance waste risk appraisal model based on modified failure mode and effect analysis (FMEA). *2016 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, 1422–1425. https://doi.org/10.1109/IEEM.2016.7798112

Thurnes, C. M., Zeihsel, F., Visnepolschi, S., & Hallfell, F. (2015). Using TRIZ to invent failures - Concept and application to go beyond traditional FMEA. *Procedia Engineering*, *131*, 426–450. https://doi.org/10.1016/j.proeng.2015.12.439

van Leeuwen, J. F., Nauta, M. J., de Kaste, D., Odekerken-Rombouts, Y. M. C.

F., Oldenhof, M. T., Vredenbregt, M. J., & Barends, D. M. (2009). Risk analysis by FMEA as an element of analytical validation. *Journal of Pharmaceutical and Biomedical Analysis*, *50*(5), 1085–1087. https://doi.org/10.1016/j.jpba.2009.06.049

Whitman, M. E., & Mattord, H. J. (2012). Principles of information security. *Course Technology*, 1–617. https://doi.org/10.1016/B978-0-12-381972-7.00002-6

Xiao, N., Huang, H. Z., Li, Y., He, L., & Jin, T. (2011). Multiple failure modes analysis and weighted risk priority number evaluation in FMEA. *Engineering Failure Analysis*, *18*(4), 1162–1170. https://doi.org/10.1016/j.engfailanal.2011.02.004

Zhao, X., & Bai, X. (2010). The application of FMEA method in the risk management of medical device during the lifecycle. *2010 2nd International Conference on E-Business and Information System Security, EBISS2010*, 455–458. https://doi.org/10.1109/EBISS.2010.5473713

Zheng, L. Y., Chin, K. S., & Wei, L. (2013). Knowledge-Enriched Process FMEA Model For Process Planning. *Asian Journal on Quality*, *3*(1), 12–27.

(Halaman ini sengaja dikosongkan)

LAMPIRAN A

Verifikasi dan Validasi Pakar

H-1. Verifikasi dan Validasi Dokumen FMEA

LEMBAR VERIFIKASI DAN VALIDASI DOKUMEN INSTRUMEN FMEA

Lembar verifikasi dan validasi dokumen instrumen FMEA ini ditujukan untuk mengesahkan bahwa daftar risiko Teknologi Informasi yang telah dirumuskan oleh peneliti telah disetujui oleh Praktisi Teknologi Informasi. Hal ini berkaitan dengan penggunaan dokumen FMEA yang digunakan untuk penilaian risiko dapat digunakan pada tahapan selanjutnya (penilaian risiko oleh kedua tim). Persetujuan dokumen instrumen FMEA nantinya akan dijadikan acuan dalam melakukan penilaian risiko. Adapun dokumen tersebut adalah skala kriteria dan daftar risiko SISKOHAT pada Bidang Penyelenggaraan Haji dan Umrah, Kantor Wilayah Kementerian Agama Provinsi Riau.

Adapun pendapat dan perbaikan daftar risiko telah dipenuhi oleh peneliti. Demikianlah surat bukti verifikasi dan validasi dokumen instrumen FMEA ini dibuat dengan sebenar-benarnya untuk dapat digunakan sebagai dokumentasi penelitian.

Pekanbaru, 10 April 2018

Disetujui oleh:

Dr. Okfalisa, S.T., M.Sc. (Praktisi risiko TI Tim 1)

Eki Saputra, S.Kom., M.Kom. (Praktisi risiko TI Tim 2)

Nina Fadilah Najwa, S.Kom. (Peneliti)

H-2. Validasi Pakar FMEA *Improvement*

LEMBAR VALIDASI *EXPERT JUDGEMENT* KERANGKA FMEA YANG DISINTESIS (FMEA *IMPROVEMENT*)

Bapak dan Ibu yang terhormat,

Saya adalah mahasiswi pascasarjana ITS Jurusan Sistem Informasi yang saat ini dalam tahapan menyelesaikan tesis, dengan judul "**Analisis Konsistensi Hasil Risiko Teknologi Informasi *Failure Mode and Effect Analysis* (FMEA)**". Penelitian ini menghasilkan metodologi peningkatan FMEA yang merupakan perbaikan dari kelemahan FMEA menghasilkan nilai inkonsistensi. Nilai inkonsistensi didapatkan dari perbedaan nilai RPN yang didapatkan pada satu studi kasus dan diukur oleh dua tim yang berbeda.

Dalam penelitian ini saya bermaksud untuk memohon kesediaan Bapak/Ibu menjadi ahli (expert). Keterlibatan Bapak/Ibu kami butuhkan dalam memberikan validasi terhadap metodologi FMEA yang telah disintesis.

Pendapat yang disampaikan oleh Bapak/Ibu akan menjadi validasi dari metodologi FMEA *Improvement*. Terima kasih banyak atas partisipasi Bapak/Ibu dalam penelitian ini.

Salam hangat,

Nina Fadilah Najwa (05211650012003)

Program Magister Jurusan Sistem Informasi

Institut Teknologi Sepuluh November

2018

LEMBAR VALIDASI *EXPERT JUDGEMENT* KERANGKA FMEA YANG DISINTESIS (FMEA *IMPROVEMENT*)

Petunjuk:

Lembar validasi ini ditujukan untuk mengetahui pendapat Bapak/Ibu sebagai ahli/*expert* terhadap metode *Failure Mode Effect and Analysis* (FMEA). Pendapat, kritik, saran dan koreksi dari Bapak/Ibu sangat bermanfaat untuk memperbaiki dan meningkatkan metodologi FMEA. Berkenaan dengan hal tersebut, saya berharap kesediaan Bapak/Ibu untuk memberikan validasi terhadap metodologi yang telah disintesis.

Pernyataan 1:

Pada Bagian ini Bapak/Ibu cukup memberikan simbol (√) pada kolom yang disediakan.

2. Dari 11 elemen yang ditentukan berdasarkan penelitian terdahulu dan standart yaitu ISO 31000 & 27001 dan ASQ apakah keseluruhannya digunakan pada proses pembuatan FMEA (berdasarkan pengalaman yang pernah dilakukan)?

No	Elemen FMEA	Ya	Tidak	Keterangan
1	Identifikasi Konteks	√		
2	Identifikasi Proses Bisnis	√		
3	Pembentukan tim FMEA	√		
4	Menentukan Metode Penilaian	√		
5	Pelatihan & Pemahaman Prosedur	√		
6	*Brainstorming* Potensi Kegagalan (*failure mode, potential effect, potential cause*)	√		
7	Penyusunan *risk register* / daftar risiko	√		
8	Pemberian nilai tingkat pada masing-masing parameter (kontrol: estimasi waktu <90 menit)	√		
9	Perhitungan RPN	√		
10	Pemrioritasan risiko	√		
11	Dokumentasi rekomendasi kontrol	√		

Berikut penjelasannya:

Nama Tahapan	Bagian Tahapan	Keterangan
Penentuan Kebutuhan Penilaian Risiko	Identifikasi Konteks	Dimana target sistem yang digambarkan dan identifikasi aset.
	Identifikasi Proses Bisnis	Memahami alur proses bisnis pada objek.
	Pembentukan tim FMEA	Menentukan pihak yang terkait dalam penilaian risiko.
	Menentukan Metode Penilaian	Skala kriteria dan desain dokumen FMEA yang telah diperbaiki.
	Pelatihan & Pemahaman Prosedur	Melakukan pelatihan kepada tim dan memberikan pemahaman prosedur penggunaan metode FMEA yang telah disintesis.
Identifikasi Risiko	*Brainstorming* Potensi Kegagalan (*failure mode, potential effect, potential cause*)	Dalam OCTAVE diketahui sebagai identifikasi aset kritis, membangun profil berbasis ancaman, profil aset berbasis ancaman, identifikasi kelemahan infrastruktur.
	Penyusunan *risk register* / daftar risiko	Mensintesis hasil *brainstorming* ke dalam pentabelan dokumen FMEA.
Analisa dan evaluasi Risiko	Pemberian nilai tingkat pada masing-masing parameter. (kontrol: estimasi waktu <90 menit)	Memberikan nilai frekuensi terjadinya risiko, nilai keparahan risiko, dan nilai deteksi risiko.
	Perhitungan RPN	Melakukan perhitungan sesuai dengan formulasi RPN.
	Pemrioritasan risiko	Mengurutkan nilai RPN dari yang besar hingga paling kecil dan membuat level risiko.
Rekomendasi Kontrol	Dokumentasi rekomendasi kontrol	Risiko yang akan dievaluasi dan dimitigasi dimasukkan kedalam dokumentasi rekomendasi kontrol.

Desain Dokumen FMEA:

Code	*Critical Assets*	*(impact) Potential Failure Modes (s)*	*Potential Effect(s) of Failure*	*SEV*	*(threat) Potential Cause(s) / Mechanism (s) of Failure*	*Source of Threat*	*OCC*	*Current Compensanting Controls* (Compensate Vulnerability)		*RPN*
								Preventive Control	*Detective Control*	
<kode aset>	<nama aset>	<dampak akhir jika terjadinya ancaman>	CIA Triad, operational.	1	Ancaman	<people, process, technology>	1	Pencegahan yang dilakukan	Monitoring	1

Skala Kriteria:

a. Kriteria Skala Tingkat Keparahan / *Severity*

Skala	Level Skala	Tingkat keparahan terhadap		
		Pelayan/operasional	Perhatian media	Finansial & Regulasi
1	Sangat Kecil	Tidak Berdampak	Tidak berdampak	Tidak Berdampak
2	Kecil	Dampak dapat diabaikan	Potensi menjadi sorotan publik	Menimbulkan kerugian finansial.
3	Sedang	Kegiatan operasional ataupun kinerja terhambat.	Pemberitaan negatif pada media massa	Sistem operasional ditembus oleh hacker/cracker
4	Besar	Pelayanan terhadap calon jemaah terganggu lebih dari 24 jam.	Ekspos utama (di media massa) lebih dari satu hari	Investigasi oleh pihak berwajib atau regulatory
5	Sangat Besar	Ketidaknyamanan yang berarti/ keresahan timbul dari seluruh calon jemaah.	Menjadi perhatian pemerintah / kehilangan kepercayaan publik	Kegagalan sistem menyeluruh / sistem secara total tidak berfungsi, kerugian finansial sangat besar.

b. Kriteria Skala Tingkat Terjadi / *Occurrence*

Skala	Level Skala	Tingkat Terjadi
1	Sangat Tidak Mungkin	Dapat diabaikan
2	Mungkin	Kecil kemungkinan terjadi
3	Kadang-kadang	Kemungkinan terjadi sedang / Bisa Terjadi
4	Hampir Pasti	Kemungkinan besar terjadi
5	Pasti Terjadi	Akan terjadi (dalam segala situasi)

c. Level Risiko

Inherent Risk		Risk Level	Action Plan
1-5	Low	Diterima	-
6-10	Low to Medium	Diterima	-
11-15	Medium	Diterima	-
16-20	Medium to High	Tidak Diterima	Dihilangkan, dikurangi, dipindahkan
21-25	High	Tidak Diterima	Dihilangkan, dikurangi, dipindahkan

Pertanyaan 3:

3. Bagaimana pendapat Bapak/Ibu mengenai metodologi FMEA yang disintesis dari penelitian ini?

Pendapat *expert*:

Penelitian ini mengidentifikasi subjektivitas pelaku evaluasi risiko sebagai penyebab utama inkonsistensi dari metode FMEA tradisional. Berdasarkan observasi ini, penelitian ini kemudian mengsisntesis perbaikan metodologi FMEA dengan beberapa langkah yang mengurangi faktor subyektivitas dalam setiap tahapan.

Pertanyaan 4:

4. Apakah menurut Bapak/Ibu, metodologi FMEA yang dihasilkan dari penelitian ini sudah mencukupi dan sesuai dengan praktik-praktik di lapangan terkait pembuatan FMEA?

Pendapat *expert*:

Tahapan dalam perbaikan metodologi FMEA yang disintesis dalam penelitian sudah sesuai dengan praktik yang umum, meskipun untuk praktik saat ini lebih banyak menggunakan COSO sebagai referensi dalam manajemen risiko.

Saran Expert:

Kriteria skala Severity dan Occurence dapat dikaji ulang untuk dapat lebih eksplisit dalam mendeskripsikan tingkat keparahan atau kemungkinan frekuensi risiko yang diidentifikasi

Surabaya, 3 Juli 2018
Validator

(Aresto Yudo Sujono)

(Halaman ini sengaja dikosongkan)

LAMPIRAN B

Prosedur Pembentukan TIM FMEA

Prosedur Pembentukan Tim FMEA

Prosedur ini dibuat berdasarkan kebutuhan dalam penelitian yang dilakukan oleh Nina Fadilah Najwa (NRP. 05211650012003), Magister Sistem Informasi, Institut Teknologi Sepuluh Nopember, Surabaya. Adapun judul penelitian adalah "Analisis Konsistensi Hasil Risiko Teknologi Informasi *Failure Mode and Effect Analysis* (FMEA)". Penelitian ini menggunakan dua siklus *action research* (*plan, act, observe, reflect*). Siklus pertama pada *action research* untuk menguji dan membuktikan konsistensi FMEA Tradisional. *Action research* yang kedua menguji coba metodologi perbaikan untuk meningkatkan konsistensi FMEA dengan mensintesis kerangka FMEA. Pengukuran risiko dilakukan oleh dua tim yang berbeda dengan satu studi kasus yang sama. Dengan adanya prosedur pembentukan tim, maka dapat membantu peneliti dalam mengukur risiko pada studi kasus yaitu Bidang Penyelenggaraan Haji dan Umrah, Kantor Wilayah Kementerian Agama Provinsi Riau. Kemudian, dengan prosedur ini membantu peneliti untuk mendapatkan komitmen dari tim yang telah ditunjuk oleh Kepala Bagian dalam menjalankan metodologi FMEA tradisional maupun FMEA yang disintesis (FMEA *Improvement*). (**Nama Tim: Terlampir**).

A. Tujuan

Penetapan tim risiko bertujuan untuk memastikan tim risiko yang melakukan penilaian risiko menggunakan metode FMEA telah memahami dan berpengalaman dalam penggunaan metode FMEA, sehingga mengurangi tingkat hasil yang tidak konsisten dalam melakukan penilaian risiko.

B. Ruang Lingkup

Ruang lingkup penetapan tim risiko adalah pihak-pihak yang terlibat dalam kegiatan manajemen risiko pada aset kritis instansi dalam penggunaan teknologi informasi menggunakan metode FMEA tradisional maupun FMEA *improvement*.

C. Indikator Kinerja

Kesesuaian waktu pelaksanaan prosedur dengan jadwal yang telah ditetapkan oleh pembuat prosedur (Instansi). Koordinator dilakukan berdasarkan kontrol dari peneliti.

D. Prosedur Pemilihan Anggota

Berikut ini adalah prosedur dalam pembentukan tim FMEA:

1. Ukuran tim 1 dan tim 2 masing-masing adalah minimal 3 orang. Rincian masing-masing tim terdiri dari peneliti, praktisi TI, pegawai Bidang Penyelenggaraan Haji dan Umrah.

2. Anggota tim dipilih berdasarkan kriteria yang telah ditentukan, yaitu:
   a. Paling sedikit ada dua teknisi ahli yang termasuk dalam tim FMEA
   b. Orang yang mengetahui tipe-tipe informasi yang berhubungan dengan aset yang terdapat dalam organisasi.
   c. Orang yang mengetahui cara mendapatkan informasi aset tersebut.
   d. Orang yang berkomitmen untuk menyediakan waktu untuk pengukuran risiko.
   e. Orang yang telah berada pada jabatannya minimal satu tahun.
   f. Memiliki otoritas untuk memilih dan memberikan perintah kepada staff untuk mengukur risiko (level manajemen).
3. Ketua tim: Seorang ketua tim harus mengontrol dan mengkoordinasi jalannya proses pengukuran risiko. Adapun hal yang harus di koordinasikan adalah:
   a. Mengatur dan memfasilitasi pertemuan termasuk jadwal dan dokumen FMEA yang akan diisi.
   b. Memastikan tim yang bersangkutan hadir.
   c. Memastikan suksesnya pengukuran risiko hingga selesai.

E. Rincian Prosedur

1. Tim risiko telah mendapatkan arahan mengenai penggunaan penilaian risiko menggunakan metode FMEA tradisional pada implementasi pertama dan FMEA *improvement* pada implementasi kedua.
2. Pihak instansi telah menunjuk dan menetapkan anggota tim risiko yang melakukan penilaian risiko pada aset kritis.
3. Tim risiko menggunakan panduan yang telah ditetapkan oleh FMEA dalam melakukan penilaian risiko pada tahapan implementasi pertama. Kemudian, mengikuti metodologi dengan kerangka FMEA yang telah disesuaikan oleh peneliti.

Mengetahui/menyetujui:

Pekanbaru, 4/7/18

Kepala Seksi SISKOHAT	Kepala Bidang Penyelenggaraan Haji dan Umrah
Drs.H.Asril	H. Erizon Efendi, S.Ag
NIP.196604112006041003	NIP.196905061996031001

LAMPIRAN

NAMA TIM FMEA YANG BERTUGAS

No	Nama	Jabatan
1.	Drs. H. Asril	KASI SUSKOHAT
2.	Nik Yustianayah	Operator/Staff SUSKOHAT

(Halaman ini sengaja dikosongkan)

LAMPIRAN C

Bukti Selesai Penilaian Risiko

H-1. FMEA Tradisional

BUKTI SELESAI PENILAIAN RISIKO FMEA

Lembar bukti penyelesaian penilaian risiko Teknologi Informasi dengan menggunakan metode FMEA ini di tanda tangani oleh tim FMEA. Berikut ini adalah jadwal pelaksanaan dari penilaian risiko:

Hari/ Tanggal : Rabu, 11 April 2018

FMEA : Tradisional

Waktu mulai : 19.00

Waktu selesai : 15.30

Nama dan daftar hadir:

No	Nama	Jabatan	Paraf
1.	Nina Fadilah Najwa	fasilitator	
2.	Nik Yusriansyah, S.Pd	operator (staff sukohati	
3.	Eki Saputra, S.Kom, M.Kom	Auditor	

Demikianlah lembar bukti ini peneliti buat sebagai kelengkapan dari prosedur dan dokumentasi untuk penelitian yang dilakukan. Terimakasih.

Pekanbaru, 11 April 2018

Peneliti,

Nina Fadilah Najwa, S.Kom

BUKTI SELESAI PENILAIAN RISIKO FMEA

Lembar bukti penyelesaian penilaian risiko Teknologi Informasi dengan menggunakan metode FMEA ini di tanda tangani oleh tim FMEA. Berikut ini adalah jadwal pelaksanaan dari penilaian risiko:

Hari/ Tanggal : Rabu, 11 April 2018

FMEA : Tradisional

Waktu mulai : 08.30

Waktu selesai : 11.30

Nama dan daftar hadir:

No	Nama	Jabatan	Paraf
1.	Nina Fadilah Najwa	fasilitator	
2.	Drs. H. Asril	KASI SISKOHAT	
3.	Dr. Okfalisa, S.T., M.Sc	Auditor	

Demikianlah lembar bukti ini peneliti buat sebagai kelengkapan dari prosedur dan dokumentasi untuk penelitian yang dilakukan. Terimakasih.

Pekanbaru, 11 April 2018

Peneliti,

Nina Fadilah Najwa, S.Kom

H-2. FMEA *Improvement*

BUKTI SELESAI PENILAIAN RISIKO FMEA

Lembar bukti penyelesaian penilaian risiko Teknologi Informasi dengan menggunakan metode FMEA ini di tanda tangani oleh tim FMEA. Berikut ini adalah jadwal pelaksanaan dari penilaian risiko:

Hari/ Tanggal : kamis, 5-7-18

FMEA : *Improvement* (FMEA yang Disintesis)

Waktu mulai : 13.40

Waktu selesai : 14.20

Nama dan daftar hadir:

No	Nama	Jabatan	Paraf
1.	Drs.H. Asril	KASI SISKOHAT	
2.	Nina Fadilah Najwa	koordinator	
3.	Dr. Okfalisa, S.T., M.Sc.	Praktisi IT	

Demikianlah, lembar bukti ini dibuat sebagai kelengkapan dari prosedur dan dokumentasi untuk penelitian yang dilakukan. Terimakasih.

Pekanbaru, 5-7-18

Peneliti,

Nina Fadilah Najwa, S.Kom

BUKTI SELESAI PENILAIAN RISIKO FMEA

Lembar bukti penyelesaian penilaian risiko Teknologi Informasi dengan menggunakan metode FMEA ini di tanda tangani oleh tim FMEA. Berikut ini adalah jadwal pelaksanaan dari penilaian risiko:

Hari/ Tanggal : Kamis, 5-7-18

FMEA : *Improvement* (FMEA yang Disintesis)

Waktu mulai : 11.00

Waktu selesai : 11.30

Nama dan daftar hadir:

No	Nama	Jabatan	Paraf
1.	NIK YUSRI	operator SISKOHAT	
2.	Eki Saputra, M.kom	Praktisi IT	
3.	Nina Fadilah Najwa	koordinator	

Demikianlah, lembar bukti ini dibuat sebagai kelengkapan dari prosedur dan dokumentasi untuk penelitian yang dilakukan. Terimakasih.

Pekanbaru, 5-7-18

Peneliti,

Nina Fadilah Najwa, S.Kom

LAMPIRAN D

Daftar Peserta Pelatihan Penilaian Risiko FMEA

DAFTAR PESERTA PELATIHAN PENILAIAN RISIKO FMEA

Lembar bukti penyelesaian pelatihan untuk memahami prosedur penilaian risiko Teknologi Informasi dengan menggunakan metode FMEA ini di tanda tangani oleh tim FMEA dan pegawai pada Bidang Penyelenggaraan Haji dan Umrah, Kantor Wilayah Kementerian Agama Provinsi Riau. Berikut ini adalah jadwal pelaksanaan dari penilaian risiko:

Pemateri : Nina Fadilah Najwa, S.Kom

Hari/ Tanggal : KAMIS, 09.00 , 5/7/18

Waktu mulai : 09.00

Waktu selesai : 10.15

Nama dan daftar hadir peserta:

No	Nama	Jabatan	Paraf
1.	NIK YUSRI	Staff / Operator SISKOHAT	
2.	Drs. H. Asril	KASI SISKOHAT	
3.	Idea Indah P	Staff PHU	
4.	Librina	Staf PHU	

Demikianlah lembar bukti ini dibuat sebagai kelengkapan dari prosedur dan dokumentasi untuk penelitian yang dilakukan. Terimakasih.

Mengetahui,
Kepala Bidang Penyelenggaraan Haji dan Umrah

H. Erizon Efendi, S.Ag
NIP. 19690506199603 1001

Pekanbaru, 5 Juli 2018
Peneliti,

Nina Fadilah Najwa
NRP. 05211650012003

(Halaman ini sengaja dikosongkan)

LAMPIRAN E

Hasil Rekapan dan Bukti Wawancara

INFORMAN 1: Kasi Pembinaan Haji dan Umrah

1. Apa saja tugas pokok dari bidang ini?
   Jawaban:

   Ada lima seksi yang ada. Pertama, seksi pendaftaran dan dokumentasi haji yang tugasnya melayani pendaftaran, semua proses dokumen keberangkatan jemaah haji. Kedua, kasi pembinaan haji dan umrah tugas pokoknya melakukan pembinaan terhadap travel haji, travel haji plus, travel umrah, dan KBIH (Kelompok Bimbingan Ibadah Haji). Kemudian melakukan manasik haji kab/kota serta petugas haji. Ketiga, Kasi SISKOHAT tugas pokok mengurusi seluruh informasi yang ada pada siskohat. Keempat, Kasi akomodasi dan transportasi, ini masalah transportasi jamaah. Terakhir, seksi keuangan haji mengurusi keuangan haji.
2. Sistem Informasi apa yang digunakan pada bidang ini dalam proses bisnisnya?
   Jawaban:

   Seluruh seksi yang ada di bidang penyelenggaraan haji dan umrah masuk ke dalam SISKOHAT. Menggunakan SISKOHAT. Untuk seksi pembinaan semua informasi travel, informasi petugas dan KBIH bisa dilihat disana.
3. Bagaimana proses implementasi sistem informasi yang ada pada bidang ini? (prosedur penggunaan SISKOHAT, ex: *password* dll)
   Jawaban:
   Semua dapat hak akses di bidang ini.
4. Siapa saja yang memiliki wewenang dalam menggunakan sistem informasi?
   Jawaban:
   Seluruh pegawai di bidang penyelenggaraan haji dan umrah. Cuma ada adminnya kan ada.
5. Seberapa pentingkah data ataupun informasi yang terdapat dalam sistem ini?
   Jawaban:
   Sangat penting sekali. Pentingnya untuk melihat informasi tentang apa yang menjadi kebijakan di pusat sama yang disini. Lebih mengontrol perjalanan travel karna travelkan online itu. Jadi bisa dilihat. Jadi lebih ke *monitoring*.
6. Apakah sudah pernah dilakukan identifikasi ancaman yang mungkin terjadi ?
   Jawaban:

Ada dari pihak pusat. Meminta masukan dari kita apa kendala kita secara keseluruhan terutama siskohat itu.

7. Apakah ada kendala selama penggunaan teknologi informasi dalam proses bisnis?
   Jawaban:

   Kendala pertama walaupun sistem jarang digunakan, kadang-kadang sistemnya suka bermasalah. Sering terjadi kelemahan pada sistem, seperti saat dibutuhkan siskohat suka tidak bisa digunakan.

8. Jika terjadi permasalahan dalam penggunaan sistem informasi, siapakah yang memiliki tanggungjawab terkait permasalahan tersebut?
   Jawab;
   Seksi siskohat. Jika masih bisa di tangani oleh operator kita maka di perbaiki. Jika tidak, seksi SISKOHAT yang melakukan koordinasi dengan kantor pusat.
9. Bagaimana kerugian finansial yang didapatkan jika terjadinya risiko teknologi informasi?
   Jawab:
   Pertama, pendaftaran kan satu orangnya 25 juta. Misalkan berapa korban yang ditimbulkan banyak juga itu.
10. Apakah ada prosedur/aturan tata cara yang telah diterapkan mengenai proteksi keamanan aset Sistem Informasi yang digunakan?
    Jawab;
11. Adakah pembatasan hak akses pengguna berkaitan dengan penjagaan keamanan aset TI?
    Jawab:
12. Apakah telah dibuat mitigasi ketika terjadi permasalahan pada keamanan aset TI yang diterapkan?
    Jawaban: Ada pada seksi SISKOHAT.
13. Apakah pernah terjadi kegagalan ataupun pengalaman terjadinya risiko disebabkan oleh ancaman? (termasuk kendala yang menghentikan proses bisnis)
    Jawaban:

    Pernah ada. Misalnya kegagalan dalam pengupdatean data. Data sudah di update disini tetapi di pusat belum masuk. Sering terjadi pada proses pembatalan. Jadi adanya keterlambatan sehari atau dua hari.

14. Bagaimana performa aset TI yang diterapkan jika akses jaringan tidak berjalan dengan baik? (lampu mati, jaringan putus)
    Jawaban:

Ya tidak bisa berjalan, kalo mati lampu ditunggu lampunya hidupnya. Kalau sistem tidak berjalan, ditunggu hingga bisa digunakan lagi. Karna perbaikan dilakukan di pusat.

15. Apakah sistem informasi yang diterapkan dapat diakses dari luar? (tidak hanya dapat diakses dari kantor)
    Jawaban:

    Bisa saja, jemaah haji yang mau lihat nomor porsi. Bisa online.

16. Dampak apakah yang mungkin timbul jika ancaman-ancaman tersebut benar-benar terjadi?
    Jawaban:

    Sebenarnya untuk seksi saya tidak terlalu ada masalah, mungkin yang sangat penting itu di seksi dokumen dan pendaftaran. Kalau sistem tidak bisa digunakan, untuk proses pembatalan, pendaftaran juga tidak dapat dilakukan.

17. Adakah ada standar keamanan yang digunakan untuk melindungi aset teknologi informasi? (contoh : ISO 27001)
    Jawaban:

    Saya kurang tahu permasalahan itu.

18. Bagaimana kondisi jaringan pada penerapan sistem informasi yang diterapkan? Pernahkah terjadi gangguan pada jaringan yang digunakan?
    Jawaban:

    Pernah, sering terjadi error dan lemah jaringan.

INFORMAN 2: Kasi SISKOHAT

1. Apa saja tugas pokok dari bidang ini?
   Jawab:

   Pertama adalah tentang pemberangkatan calon jemaah haji dan umrah. Kedua, tentang proses *monitoring* pelaksanaan ibadah umrah dan haji khusus. Jadi secara garis besar haji diberangkatkan oleh pemerintah dalam hal ini kementerian agama. Kemudian, proses pendaftaran sampai dengan pemberangkatan. Kemudian, proses pemberangkatan jemaah umrah dilaksanakan travel agent dan sama dengan jemaah haji khusus dilaksanakan travel agent. Travel yang memiliki izin.

2. Sistem Informasi apa yang digunakan pada bidang ini dalam proses bisnisnya?
   Jawab:

SISKOHAT Gen 2.

3. Bagaimana proses bisnis yang ada pada bidang ini? (masing-masing seksi, dalam menggunakan SISKOHAT)
   Jawab:

   Siskohat ini kita harus memiliki *password*nya apa. Untuk meihat nomor porsi, bisa di lihat di situs kemenag yang terhubung dengan Siskohat. Untuk fungsi siskohat di kasi siskohat menginformasikan tentang calon-calon jemaah haji yang berangkat tahun berikutnya, media elektorinik, media masa dan lainnya. Menyampaikan informasi menyangkut dengan haji disampaikan pada kemenag kab/kota atau ada kebijakan kemenag disampaikan.

4. Aset-aset TI apa sajakah yang mendukung berjalannya sistem informasi yang ada pada bidang ini? (*hardware*, *software*, data, network), sebutkan peranannya.
   Jawab:
   Masalah aset yang dipergunakan dalam hal proses pemberangkatan jemaah haji tentu ada PC, TI, fasilitas yang mendukung seperti internet, microsoft word.
5. Bagaimana proses implementasi sistem informasi yang ada pada bidang ini? (prosedur penggunaan SISKOHAT, ex: *password* dll)
   Jawab:
   Kalau di haji, boleh semua mengakses SISKOHAT. Diberikan *password* dan usernamenya, biasanya di tempel saja di komputer.
6. Seberapa pentingkah data ataupun informasi yang terdapat dalam sistem ini?
   Jawab:
   Kalau masalah data, datanya yang ada diakses di dalam siskohat. Ada data haji reguler, haji khusus, sudah terdaftar atau belum, jadwal keberangkatan, nomor porsi, persyaratan pendaftaran, pembatalan haji, keuangan yang setelah diaudit.
7. Apakah sudah pernah dilakukan identifikasi ancaman atau penilaian risiko yang mungkin terjadi ?
   Jawab:
   Identifikasi risiko IT belum pernah dilakukan.
8. Apakah ada kendala selama penggunaan teknologi informasi dalam proses bisnis?
   Jawab:

   Sering terjadinya error. Permasalahannya pada jaringan pusatnya. Biasanya terjadi kendala itu dari pihak pusat. Jika ada kendala maka seluruhnya tidak bisa akses. Terkadang memang lelet jaringannya.

9. Jika terjadi permasalahan dalam penggunaan sistem informasi, siapakah yang memiliki tanggungjawab terkait permasalahan tersebut?
   Jawab:
   Segala kesalahan ataupun masalah, maka tanggungjawab kepada seksi siskohat.
10. Bagaimana kerugian finansial yang didapatkan jika terjadinya risiko teknologi informasi?
    Jawab:
    Kerugian yang didapatkan karena sistem tidak dapat digunakan adalah dari secara materi mungkin tidak ada. Tetapi dari segi pelayanan iya. Kalau ada calon jemaah yang bertanya dan datang ke Kemenag Riau saat sistem tidak bisa diakses.
11. Apakah telah diterapkan penjadwalan untuk melakukan pemeriksaan pada keamanan?
    Jawab:

    Untuk maintenance dilakukan 1 tahun sekali dari pusat untuk melihat alat-alat siskohat. Kalau ada perbaikan di off kan dulu.

12. Adakah pembatasan hak akses pengguna berkaitan dengan penjagaan keamanan aset TI?
    Jawab:

    Hanya pegawai bidang penyelenggaraan haji dan umrah saja yang bisa akses.

13. Apakah telah dibuat mitigasi ketika terjadi permasalahan pada keamanan aset TI yang diterapkan?
    Jawab:

    Menjalani saja apa yang ada sekarang.

14. Apakah pernah terjadi kegagalan ataupun pengalaman terjadinya risiko disebabkan oleh ancaman? (termasuk kendala yang menghentikan proses bisnis)
    Jawab:

    Sering error. Kalau ada kerusakan 2 hingga 3 jam. Kalau siskohat tidak bisa di akses, di bank juga tidak bisa diakses.

15. Apakah pernah dilakukan identifikasi mengenai ancaman yang mungkin terjadi terkait penerapan teknologi informasi?
    Jawab:

    Belum pernah.

16. Bagaimana performa aset TI yang diterapkan jika akses jaringan tidak berjalan dengan baik? (lampu mati, jaringan putus)
    Jawab:

Ditunggu saja hingga bisa diakses kembali.

17. Apakah ada panduan bagi karyawan (pengguna) mengenai ancaman yang mungkin terjadi pada penggunaan TI?
    Jawab:

    Tidak ada

18. Praktek apa saja yang telah dilakukan dalam melakukan proteksi keamanan aset TI?
    Jawab:

    Keamanan yang sudah diterapkan saat ini, ada kunci komputer masing-masing. Untuk cara ganti *password* harus izin ke pusat dulu.

INFORMAN 2: Operator SISKOHAT

Pertanyaan Identifikasi Proses Bisnis

Pertanyaan yang diajukan menggali proses bisnis yang ada pada bidang yang diajukan. Adapun pertanyaan yang diajukan adalah:

1. Apa saja tugas pokok dari bidang ini?
   Jawab:

   Pendaftaran haji khusus di kemenag provinsi, pendaftaran haji reguler di kemenag kab/kota. Biasanya *monitoring* data jemaah haji per bulan.

2. Sistem Informasi apa yang digunakan pada bidang ini dalam proses bisnisnya?
   Jawab:

   SISKOHAT digunakan oleh semua staff bidang penyelenggaraan haji dan umrah, KASI, dan memiliki dua operator utama. Kalau ada perbaikan data dilakukan oleh kemenag RI, untuk permintaan perbaikan. Apabila semakin banyak surat perbaikan, maka tidak profesional. Adapun proses pendaftaran haji itu adalah jemaah ke Bank untuk membayar uang pangkal sebesar 25 juta, lalu Bank akan memberikan lembar validasi. Syaratnya adalah usia minimal 12 tahun, KTP domisili, uang setoran, buku tabungan. Lembar validasi dibawa oleh jemaah kepada Kemenag. Lalu diinputkan dan dapat nomor porsi. SISKOHAT itu ada 3, SISKOHAT Kemenag, SISKOHAT Bank, SISKOHAT Kesehatan. Kita bisa melakukan cek, data jemaah haji bayarnya berapa melalui Bank itu.

Pertanyaan Profil Aset Berbasis Ancaman.

Aspek 1. Aset Kritis Teknologi Informasi

Pertanyaan pada aspek 1 ini untuk menggali aset-aset kritis (sistem atau teknologi informasi) yang ada dalam proses bisnis. Berikut ini adalah daftar pertanyaan yang diajukan:

1. Aset-aset TI apa sajakah yang mendukung berjalannya sistem informasi yang ada pada bidang ini? (*hardware*, *software*, data, network), sebutkan peranannya.
   Jawab:
   Komputer PC, pendaftaran haji yang diperlukan finger print dan kamera. *Scanner* juga diperlukan. Untuk *server* kita menggunakan VPN dari pusat yang hanya dapat mengakses siskohat. Baik wifi maupun LAN. UPS tidak ada, genset juga tidak ada. Karena kita berada di jaringan protokoler. Tidak ada pencegahan mati lampu. Antivirus digunakan adalah avast dan avg. Sistem operasi *windows* 7 dan 10. *Server* kita ada inmas, IBM yang terletak di lantai bawah. *Software* yang digunakan adalah java disesuaikan dengan kebutuhan siskohat dan untuk menampilkan data fingerprint dan fotonya.
2. Bagaimana proses implementasi sistem informasi yang ada pada bidang ini? (prosedur penggunaan SISKOHAT, ex: *password* dll).
   Jawab:
   12 kemenag kab kota mendapatkan VPN. Termasuk provinsi jadinya 13. VPN sudah kita pasang langsung di perangkat. Diluar situs siskohat tidak bisa diakses. Kita menerima yang sudah jadi.
3. Apakah ada prosedur yang memberikan penjelasan mengenai implementasi sistem atau teknologi informasi?
   Jawab:
   Operator pendaftaran dan pembatalan. Disini menjadi satu fungsi karena sedikit pegawai. Misal di jawa timur, satu pendaftaran bisa tiga operator.
4. Siapa saja yang memiliki wewenang dalam menggunakan sistem informasi?
   Jawab:
   Staff haji dan seksi siskohat. KASI menjalankan fungsi *monitoring*.
5. Seberapa pentingkah data ataupun informasi yang terdapat dalam sistem ini?
   Jawab:
   Data yang ada pada siskohat itu data jemaah haji yang lengkap, estimasi keberangkatan, untuk melihat nomor porsi bisa dilihat pada situs kemenag. Perbaikan kesalahan biodata dapat dilakukan hanya dapat dirubah oleh orang pusat. Sangat penting sekali. Ada 85.000 calon jemaah haji riau, di bagi dengan 5000 kuota riau, sehingga satu orang menunggu 17 tahun keberangkatan haji. Maka data itu harus di proteksi.
6. Apakah sudah pernah dilakukan identifikasi ancaman yang mungkin terjadi ?

Jawab:

Belum pernah.

7. Apakah ada kendala selama penggunaan teknologi informasi dalam proses bisnis?
   Jawab:

   Tidak ada. Paling jaringan saja.

8. Jika terjadi permasalahan dalam penggunaan sistem informasi, siapakah yang memiliki tanggungjawab terkait permasalahan tersebut?
   Jawab:
   Seksi SISKOHAT.

Aspek 2. Mengidentifikasi Kebutuhan Keamanan Aset

Pertanyaan pada aspek 2 ini berguna untuk menggali informasi mengenai penerapan proteksi keamanan pada Teknologi Informasi yang diterapkan pada studi kasus. Adapun pertanyaan yang diajukan adalah:

1. Teknologi Informasi apa saja yang digunakan untuk melakukan proteksi pada keamanan aset Sistem Informasi yang digunakan? (aplikasi/jaringan/teknologi)
   Jawab:

   Menggunakan jaringan VPN, menggunakan dua layer dalam mengakses SISKOHAT. Kemudian, adanya pemblokiran akun jika salah memasukkan *password* sebanyak 3 kali.

2. Apakah ada prosedur/aturan tata cara yang telah diterapkan mengenai proteksi keamanan aset Sistem Informasi yang digunakan?
   Jawab:

   Setahun sekali ganti *password*. Kalo 3 kali kesalahan langsung di blokir. Kalau ingin ganti *password* koordinasi ke pusat untuk permintaan pergantian *password*.

3. Apakah telah diterapkan penjadwalan untuk melakukan pemeriksaan pada keamanan?
   Jawab:

   Untuk maintenance biasanya sekali dalam 6 bulan, tetapi hanya *monitoring* saja. Untuk pemeriksaan secara menyeluruh sekali dalam setahun.

4. Adakah pembatasan hak akses pengguna berkaitan dengan penjagaan keamanan aset TI?
   Jawab:

Hanya orang-orang yang memiliki link VPN, username dan *password* yang bisa mengakses siskohat. Dan diakses di wilayah kantor.

5. Apakah telah dibuat mitigasi ketika terjadi permasalahan pada keamanan aset TI yang diterapkan?
   Jawab:

   Belum ada secara prosedural.

Aspek 3. Identifikasi Ancaman Aset Kritis

Pertanyaan pada aspek 3 bertujuan untuk menggali informasi ancaman penerapan Teknologi Informasi yang mungkin terjadi pada studi kasus. Adapun pertanyaan yang diajukan adalah:

1. Apakah pernah terjadi kegagalan ataupun pengalaman terjadinya risiko disebabkan oleh ancaman? (termasuk kendala yang menghentikan proses bisnis)
   Jawab:

   Ada pernah kehilangan. Tetapi tidak di bidang ini. Di bidang lain. kalau sekarang sudah dikasih batas siapa yang boleh masuk. Seperti area yang dibatasi tidak boleh orang lain yang tidak memiliki izin masuk. Terlebih dahulu ke bagian depan untuk izin menemui siapa. Karena sudah adanya sekat-sekat atau batas ruangan.

2. Apakah pernah dilakukan identifikasi mengenai ancaman yang mungkin terjadi terkait penerapan teknologi informasi?
   Jawab:

   Belum Pernah

3. Apakah telah dilakukan antisipasi pada ancaman yang mungkin terjadi terhadap aset TI yang diterapkan?
   Jawab:

   Ya, sudah ada.

4. Bagaimana performa aset TI yang diterapkan jika akses jaringan tidak berjalan dengan baik? (lampu mati, jaringan putus)
   Jawab:

   Kita tidak memiliki UPS ataupun genset mengingat berada di jalur protokoler.

5. Apakah ada panduan bagi karyawan (pengguna) mengenai ancaman yang mungkin terjadi pada penggunaan TI?
   Jawab:

   Tidak ada.

6. Bagaimana persiapan mitigasi apabila terjadi bencana alam terkait aset TI yang ada?
   Jawab:

   Sejauh ini tidak ada ya, karena belum pernah terjadi bencana alam. Persiapan mitigasi hanya memanfaatkan cadangan perangkat. Telah ada disediakan 5 laptop jika ada kerusakan PC.
7. Apakah sistem informasi yang diterapkan dapat diakses dari luar? (tidak hanya dapat diakses dari kantor)
   Jawab:

   VPN itu hanya IP address yang sudah terdaftar yang dapat mengakses. Sehingga, tidak dapat diakses di luar kantor.

Aspek 4. Identifikasi keamanan yang sudah diterapkan.

Pertanyaan pada aspek 4 bertujuan untuk mengidentifikasi informasi yang diterapkan pada praktek proteksi keamanan aset Teknologi Informasi. Berikut ini adalah daftar pertanyaan yang diajukan:

1. Praktek apa saja yang telah dilakukan dalam melakukan proteksi keamanan aset TI?
   Jawab:

   Yang jelas saat sekarang ini gedung kita satu pintu masuk. Sudah ada satpamnya. Dan selesai jam kantor ruangan dikunci dan tidak ada yang boleh masuk kecuali cleaning service. Adapun orang luar masuk, harus menemui orang yang menjaga di counter. Kalau untuk siskohat, masing-masing pc ada *password*nya. Untuk situs, kemenag pusat yang memproteksi. Dari sisi jaringan, kita ada dua *password*. Pertama kita masuk ke jaringan, kedua *password* untuk masuk ke situs. Karena VPN itu hanya IP address yang sudah terdaftar yang dapat mengakses. Sehingga, tidak dapat diakses di luar kantor.

   Setiap jam 4 sore selalu ada pengumuman untuk mengingatkan untuk mematikan komputer ataupun perangkat. Maintenance nya biasanya 6 bulan sekali, dan misalnya ada kerusakan kita akan langsung perbaiki. Karena untuk sistemnya sendiri sudah diatur dan diproteksi langsung oleh kemenag pusat.
2. Adakah panduan bagi karyawan terkait dengan penerapan praktek keamanan aset TI?
   Jawab:

Tidak ada panduan. Hanya ada meeting, jikalau ada perubahan ataupun penambahan modul-modul.

3. Adakah ada standar keamanan yang digunakan untuk melindungi aset teknologi informasi? (contoh : ISO 27001)
   Jawab:

   Sepertinya ada, kalau tidak salah dokumennya ada di bagian umum.

Aspek 5. Identifikasi Kelemahan Organisasi

Pertanyaan pada aspek 5 bertujuan untuk mengidentifikasi kelemahan aset sistem informasi dan infrastruktur yang ada. Berikut ini adalah daftar pertanyaan yang diajukan:

1. Bagaimana kondisi ruangan yang terdapat aset teknologi informasi?
   Jawab:

   Ada CCTV. Kebijakan kantor untuk proteksi adanya partisi ruangan.

2. Adakah kebijakan khusus dari instansi demi mengatur kondisi pada ruangan terkait dengan keamanan atau hak akses?
   Jawab:

   Adapun orang luar masuk, harus menemui orang yang menjaga di counter. Sudah adanya sekat-sekat atau batas ruangan.

3. Adakah sistem yang mampu mendeteksi masalah yang mungkin timbul sebelum masalah tersebut terjadi?
   Jawab:

   Ya sudah ada. *Windows* kita tanpa sengaja kita update, sehingga SISKOHAT ini kan jarang sekali ada update. Nah itu kita mengembalikan ke versi sebelumnya. Paling umum cocok ke *windows* 7. Jika *windows* 10 itu harus ada penyesuaian lagi dengan aplikasi lain yang mendukung.

4. Apakah seluruh sistem informasi terhubung dengan Kantor Kementerian Agama RI? Bagaimana jika terjadi gangguan jaringan?
   Jawab:

   Iya. Kita sudah siapkan nomor operator pusat. Kita memiliki whatsapp dan surat. Biasanya ada pemberitahuan dari pusat jika SISKOHAT tidak dapat digunakan dan dalam tahap maintenance.Biasanya maintenance dilakukan di atas jam kerja.

Pertanyaan Identifikasi Kelemahan Infrastruktur

Aspek 1. Komponen Kunci

Pertanyaan aspek 1 pada bagian identifikasi kelemahan infrastruktur bertujuan untuk mengidentifikasi aset teknologi informasi yang diterapkan. Berikut ini adalah daftar pertanyaan yang terkait aspek komponen kunci:

1. Bagaimana kondisi jaringan pada sistem informasi yang diterapkan? Apakah tersambung ke seluruh kantor cabang atau hanya ke kantor pusat?
   Jawab:

   12 kemenag kab kota mendapatkan VPN. Termasuk provinsi jadinya 13. VPN sudah kita pasang langsung di perangkat. Diluar situs siskohat tidak bisa diakses. Semua terhubung ke SISKOHAT pusat.
2. Apakah Kantor Wilayah Kementerian Agama Provinsi Riau telah memiliki ganset jika terjadi lampu mati? Sudah memiliki UPS?
   Jawab:

   UPS tidak ada, genset juga tidak ada. Karena kita berada di jaringan protokoler. Tidak ada pencegahan mati lampu.
3. Bagaimana langkah yang dilakukan jika terjadi gangguan pada jaringan?
   Jawab:

   Biasanya kita langsung menelepon ke kantor pusat. Jika kantor pusat tidak dapat menyelesaikan masalah, maka kantor pusat akan mengontak telkom pekanbaru dan orang telkom yang mengutus utusannya kesini.
4. Bagaimana kontrol terhadap aset-aset teknologi informasi yang ada?
   Jawab:

   Dari segi ruangan sudah ada partisi, penggunaan pendingin ruangan, memberikan *password* pada masing-masing PC, dan mematikan seluruh perangkat teknologi saat meninggalkan ruangan.

Aspek 2. Identifikasi Kelemahan Infrastruktur

Pertanyaan aspek 2 bertujuan untuk mengidentifikasi kelemahan infrastruktur yang ada pada studi kasus. Berikut ini adalah hal-hal yang diajukan pada studi kasus:

1. Bagaimana kondisi jaringan pada penerapan sistem informasi yang diterapkan? Pernahkah terjadi gangguan pada jaringan yang digunakan?
   Jawab:

   Baik, hanya gangguan dari kecepatan akses.

2. Bagaimana jika terjadi gangguan pada jaringan atau terjadi lampu mati? Berapa lama waktu yang dibutuhkan untuk memulihkan kondisi?
   Jawab:

   Tidak ada penanganan khusus. Tidak ada genset ataupun UPS. Hal ini dikarenakan lokasi kemenag riau berada pada jalur protokoler yang listriknya tidak ada mati lampu.
3. Pernahkah terjadi gangguan pada *server*? Bagaimana tindakan cepat yang dilakukan?
   Jawab:

   Kalau sekarang tidak ada.
4. Bagaimana kondisi penataan kabel yang ada? Apakah benar-benar aman dan tidak menimbulkan ancaman konsleting?
   Jawab: rapih. Dan aman insyaallah. Kalau yang kabel diatas ini itu orang telkom yang memasang, kita tidak tahu kapan mereka memasangnya. Tetapi masih tidak terganggu.
5. Bagaimana kondisi suhu ruangan apakah telah sesuai dengan penggunaan aset TI sehingga tidak menimbulkan ancaman *hardware* TI menjadi panas dan terbakar?
   Jawaba:

   Baik. Dan kondisi ruangan tidak terlalu dingin dan tidak panas. Sudah ada AC.

Pertanyaan Mengembangkan Strategi & Perencanaan Keamanan

Aspek 1. Risiko pada Aset Kritis

Pertanyaan pada aspek ini untuk menggali informasi risiko yang dapat muncul dari aset teknologi yang telah di terapkan pada studi kasus. Berikut ini adalah daftar pertanyaan yang diajukan pada studi kasus:

1. Apakah para pegawai mengikuti praktek proteksi keamanan yang berlaku di organisasi?
   Jawab:

   Iya, setiap apel pagi selalu ada arahan terkait penggunaan teknologi informasi yang aman. Dan tiap sore selalu ada pengumuman untuk mematikan perangkat sebelum pulang.
2. Bagaimana pegawai melakukan kontrol terhadap teknologi informasi yang mereka gunakan?
   Jawab:

Mematikan perangkat saat meninggalkan ruangan.

3. Adakah pegawai yang menyalahgunakan hak akses yang didapatkan?
   Jawab:

   Pada intinya, selagi tidak mengganggu tidak masalah. Contohnya selagi membuka SISKOHAT, bisa membuka email. Tetapi membuka situs seperti youtube tidak bisa. Sudah adanya kode etik pegawai untuk menjaga informasi negara. Jika ada kebocoran bisa diberhenntikan operatornya. Ada 5 poin yang salah satunya menjaga rahasia jabatan. Sehingga tidak bisa semena-mena. Jika ada media yang meminta informasi, harus melalui kepala bidang, dan yang mengomentari juga kepala bukan operator.

4. Apakah Kantor Wilayah Kementerian Agama memiliki prosedur atau kebijakan terkait pemetaan risiko aset-aset kritis?
   Jawab:

   Kalau kita ada di bagian akomodasi. Masing-masing bidang punya akomodasi. Seperti kita memiliki asrama haji,dan masing-masing itu dikelola oleh sekretaris jendral. Jadi, kita disini sebagai pelaksana.

5. Apakah terdapat identifikasi otorisasi terhadap aset informasi perusahaan?
   Jawab:

   Wajib, harus adanya jenjang. Atas persetujuan atasan dalam menginformasikan. Kebanyakan selama ini biasanya media menanyakan jumlah keberangkatan saja.

6. Adakah serangan dari pihak luar terkait pencurian informasi, pembobolan sistem, ataupun penyerangan virus?
   Jawab:

   Selama ini tidak ada. Yang ada itu, website berita yang menjelekkan institusi kami.

Aspek 2. Pengukuran Risiko

Pertanyaan pada aspek ini menyangkut pengukuran risiko TI yang mungkin terjadi pada penggunaan TI. Berikut ini adalah daftar pertanyaan yang diajukan:

1. Apakah terdapat standar pengukuran risiko?
   Jawab:

   Tidak ada.

2. Apakah terdapat prosedur dokumentasi otorisasi dan pengawasan karyawan dalam penyediaan informasi?

Jawab:

Ada, ada jenjangnya. Jadi dimulai dari Kepala Bidang meminta informasi dari SISKOHAT melalui KASI SISKOHAT, lalu KASI SISKOHAT meminta kepada operator SISKOHAT.

3. Apakah standar operasional sesuai dengan standar yang berlaku dengan yang diterapkan oleh Kantor Wilayah Kementerian Agama RI?
   Jawab:

   Sudah sesuai. Seperti pelayanan kepada jemaah haji yang datang meminta informasi estimasi keberangkatan dan pembatalan maksimal dilayani 5 menit per orangnya.

Aspek 3. Strategi Proteksi

Pertanyaan pada aspek ini bertujuan untuk melihat kesesuaian strategi dengan perlindungan sistem yang ada. Berikut ini adalah daftar pertanyaan yang diajukan:

1. Apakah strategi bisnis instansi mempertimbangkan keamanan informasi?
   Jawab:

   Iya sudah tentunya.

2. Apakah strategi keamanan didokumentasikan dan ditinjau secara rutin?
   Jawab:

   Kita mendokumentasikannya melalui banner-banner yang dikirimkan ke kab/kota. Sebagai standar layanan kita.

3. Apakah strategi keamanan diperbaharui secara berkala dalam instansi?
   Jawab:
   Kalaupun ada biasanya di beritahukan dari pusat.
4. Apakah strategi keamanan dan kebijakan dipertimbangkan dalam strategi bisnis dan tujuan instansi?
   Jawab:

   Iya sudah.

Aspek 4. Rencana Mitigasi Risiko

Pertanyaan pada aspek ini bertujuan untuk mengetahui apakah pada Kantor Wilayah Kementerian Agama telah merencanakan tindak mitigasi risiko TI. Berikut adalah pertanyaan yang diajukan:

1. Apakah terdapat pendokumentasian terkait penanggulangan dan pencegahan risiko?
   Jawab:

Risikonya tidak ada, Cuma terlambat saja. Sehingga, kita hanya melayani dan melihat kepuasan dari calon jemaah haji saja.

2. Bagaimana proses menanggapi pelanggaran keamanan?
   Jawab:

   Kalau selama ini hanya dari segi keuangan, misalnya AC tidak dimatikan ataupun adanya pembengkakan biaya listrik di bagian kita. Nantinya akan ditanyakan atau dievaluasi, mengapa bisa terjadi kenaikan oleh Subbag Umum.

3. Bagaimana proses *monitoring* terhadap keamanan TI?
   Jawab:

   Biasanya dilakukan oleh cleaning service yang melakukan cek-cek ruangan dan lampu. *Monitoring* umum yang dilakukan pusat biasanya 1 kali dalam setahun.

4. Apakah terdapat back up data yang berhubungan dengan operasional instansi?
   Jawab:

   Pasti ada, baik di kita ataupun di pusat. Jadi data itu tidak akan hilang. Seingat saya di pusat itu terdapat empat *server*. Itulah yang menampung data jemaah haji. *Server* disini itu gunanya sebagai pendorong saja.

5. Bagaimana proses pemantauan kerusakan sistem?
   Jawab:

   Langsung eksekusi saja. Kalau sifatnya urgent, maka akan dihubungi pusat. Kalau tidak, kita bisa selesaikan sendiri. Sehingga, setiap tahun selalu ada pelatihan pegawai terkait SISKOHAT. Proteksi data dengan menyimpan data-data jemaah haji seluruhnya agar menghindari double keberangkatan.

Bukti Wawancara

PROFIL INFORMAN

1. Nama Instansi : KANTOR WILAYAH KEMENTERIAN AGAMA PROV. RIAU BIDANG PENYELENGGARAAN HAJI DAN UMRAH
2. Tanggal dan waktu Interview : Senin, 2 APRIL 2018
3. Nama : Drs. H. Asril
4. Jabatan : KASI SISKOHAT
5. Lama Kerja : 5 tahun
6. Kualifikasi :
   - mengetahui proses bisnis SISKOHAT
   - KASI SISKOHAT
   - Bekerja lebih dari 1tahun.

Pekanbaru, 2 April 2018

Drs. H. Asril

PROFIL INFORMAN

1. Nama Instansi : KANTOR WILAYAH KEMENTERIAN AGAMA PROV. RIAU BIDANG PENYELENGGARAAN HAJI DAN UMRAH.

2. Tanggal dan waktu Interview : Senin, 2 April 2018

3. Nama : NIK YUSRI

4. Jabatan : staff SISKOHAT

5. Lama Kerja : 15 tahun

6. Kualifikasi :
- mengetahui proses bisnis bidang penyelenggaraan haji & umrah
- operator
- berpengalaman

Pekanbaru, 2 APRIL 2018

NIK YUSRI

PROFIL INFORMAN

1. Nama Instansi : KANTOR WILAYAH KEMENTERIAN AGAMA. PROVINSI RIAU
BIDANG PENYELENGGARAAN HAJI DAN UMRAH.

2. Tanggal dan waktu Interview : Kamis, 29 Maret 2018

3. Nama : Abdul Wahid

4. Jabatan : Kasi Pembinaan Haji dan Umrah

5. Lama Kerja : Januari 2015

6. Kualifikasi :
- menggunakan SISTEMKAT
- mengetahui alur proses bisnis.

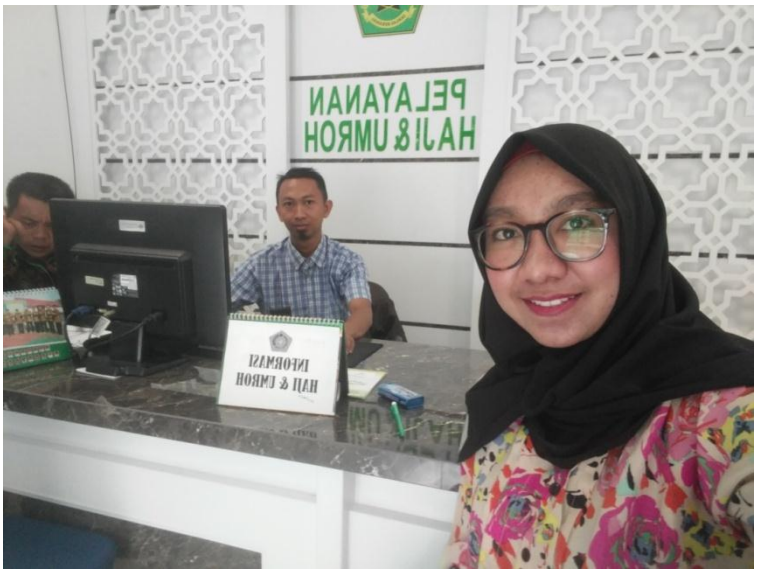
Pekanbaru, 29 Maret 2018

ABDUL WAHID

(Halaman ini sengaja dikosongkan)

LAMPIRAN F

Dokumentasi Implementasi Kerangka FMEA Tradisional dan FMEA *Improvement*




PELA
HAJI&

LAMPIRAN G

Tabel Korelasi

1. Pengolahan Data *Action Research* 1

Correlations

		RPN1	RPN2
RPN1	Pearson Correlation	1	.848**
	Sig. (2-tailed)		.000
	N	37	37
RPN2	Pearson Correlation	.848**	1
	Sig. (2-tailed)	.000	
	N	37	37

**. Correlation is significant at the 0.01 level (2-tailed).

2. Pengolahan Data *Action Research* 2

Correlations

		RPN1	RPN2
RPN1	Pearson Correlation	1	.937**
	Sig. (2-tailed)		.000
	N	37	37
RPN2	Pearson Correlation	.937**	1
	Sig. (2-tailed)	.000	
	N	37	37

**. Correlation is significant at the 0.01 level (2-tailed).

(Halaman ini sengaja dikosongkan)

BIODATA PENULIS

Nina Fadilah Najwa, lahir di Pekanbaru pada tanggal 30 Mei 1994. Penulis telah menempuh pendidikan formal di SDN 017 Bukit Raya Pekanbaru, MTsN Pekanbaru, dan MAN 2 Model Pekanbaru. Pada tahun 2012 penulis melanjutkan pendidikan jenjang S1 Program Studi Sistem Informasi pada Universitas Islam Negeri Sultan Syarif Kasim Riau. Pada tahun 2016 penulis berhasil menyelesaikan studi S1 dengan tugas akhir yang berjudul "Analisis Penerimaan Sistem Komputerisasi Haji Terpadu (SISKOHAT) Menggunakan Metode TAM (Studi kasus: Kantor Wilayah Kementerian Agama Provinsi Riau". Pada tahun 2017 penulis memperoleh Beasiswa Unggulan *on going* dari Kementerian Pendidikan dan Kebudayaan Republik Indonesia untuk melanjutkan pendidikan jenjang S2 di Program Magister Sistem Informasi, Institut Teknologi Sepuluh Nopember. Pada penelitian tesis ini, penulis mengambil konsentrasi Manajemen Sistem Informasi (MSI) dengan topik Manajemen Risiko. Kritik dan saran yang membangun dapat disampaikan melalui nina.fadilah.najwa16@mhs.is.its.ac.id atau ninafadilahnajwa@gmail.com.